European
Commission

JRC CONFERENCE AND WORKSHOP REPORT

Critical Service continuity, Resilience and Security: Proceedings of the 56th ESReDA Seminar

Hosted by the Johannes Kepler University, Linz, Austria
May 23-24, 2019

Žutautaitė, I, Eid, M., Simola, K., Kopustinskas, V.

2019

ESReDA
European Safety, Reliability & Data Association

Joint
Research
Centre

EUR 29989 EN

This publication is a Conference and Workshop report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

EU Science Hub
https://ec.europa.eu/jrc

JRC118427

EUR 29989 EN

PDF ISBN 978-92-76-13359-9 ISSN 1831-9424 doi:10.2760/23760

Luxembourg: Publications Office of the European Union, 2019.

How to cite this report: Žutautaitė, I, Eid, M., Simola, K., Kopustinskas, V., *Critical Service continuity, Resilience and Security: Proceedings of the 56th ESReDA Seminar Hosted by the Johannes Kepler University, Linz, Austria May 23-24, 2019*, EUR 29989 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-13359-9, doi:10.2760/23760, JRC118427.

European Safety, Reliability & Data Association

(ESReDA)

European Safety, Reliability & Data Association (ESReDA) is a European Association established in 1992 to promote research, application and training in Reliability, Availability, Maintainability and Safety (RAMS). The Association provides a forum for the exchange of information, data and current research in Safety and Reliability.

The contents of ESReDA seminar proceedings do not necessarily reflect the position of ESReDA. They are the sole responsibility of the authors concerned. ESReDA seminar's proceedings are designed for free public distribution. Reproduction is authorized provided the source is acknowledged.

ESReDA membership is open to organisations, privates or governmental institutes, industry researchers and consultants, who are active in the field of Safety and Reliability. Membership fees are currently 1000 EURO for organisations and 500 EURO for universities and individual members. Special sponsoring or associate membership is also available.

For more information and available ESReDA proceedings please consult:
http://www.esreda.org/

Table of contents

Preface

Critical Infrastructures (CIs) remain among the most important and vital service providers to modern societies. Severe CIs' disruptions may endanger security of the citizen, availability of strategic assets and even the governance stability. Not surprisingly, CIs are often targets of intentional attacks, either of physical or cyber nature. Newly emerging hybrid threats primarily target CIs as part of the warfare.

Resilience of CIs is addressed by a growing number of researchers and research centres, discussed by the governments and at international organisations. The European Commission is currently reviewing the Directive 2008/114/EC on the identification and designation of European CIs. Recently the Joint Research Centre (JRC) which is the European Commission's science and knowledge service has completed a pilot study within the European Programme for European Critical Infrastructure Protection (EPCIP) to address risk assessment methodology and application to a selected EU energy network comprising both gas and electricity supply. The work performed and lessons learned led to identification of a number of remaining challenges in the area that were presented during the 56th ESReDA Seminar.

Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe is a topic of the EU funded research programme H2020 for several recent calls. Just to name a few successful applications, research is being performed under SATIE, SAURON, STOP-IT, SECURE-GAS, DEFENDER and other CIs related projects.

ESReDA as one of the most active EU networks in the field has initiated a project group (CI-PR/MS&A-Data) on the "Critical Infrastructure/Modelling, Simulation and Analysis – Data". The main focus of the project group is to report on the state of progress in MS&A of the CIs preparedness & resilience with a specific focus on the corresponding data availability and relevance. In order to report on the most recent developments in the field of the CIs preparedness & resilience MS&A and the availability of the relevant data, ESReDA held its 48th, 52nd and 56th Seminars.

The 56th ESReDA Seminar on "Critical Services continuity, Resilience and Security" attracted about 30 participants from industry, authorities, operators, research centres and academia. The seminar programme consisted of 18 technical papers, two plenary speeches and an interactive session on Climate & CI protection.

The editorial work for this volume was supported by the Joint Research Centre of the European Commission in the frame of JRC support to ESReDA activities. A special thanks is due to A. Liessens (JRC) for the editorial work.

Dr. Dmitry Efrosinin	Dr. Vytis Kopustinskas, Dr. Kaisa Simola
Johannes Kepler University	EC Joint Research Centre

Dr. Mohamed Eid

Commissariat for Atomic Energy & Alternative Energies

Risk and Reliability Engineering for Crisis Management: Using Experience from Asset Management

Cyp F.H. van Rijn, Lecturer Risk Assessment and Safety, Master of Engineering, Utrecht University of Applied Sciences,
Hon. President ESReDA

Abstract

History shows that scientific research in Risk and Reliability Engineering has not been very successful in improving Asset Management whilst a comparable disciple as control engineering is now fully integrated into the (process) engineering curriculum and widespread applied.

The author has 20 years' experience of teaching some 300 Master students, trying to close the intellectual gap between (stochastic) Operations Researchers and practical (especially, mechanical) engineers.

Discussing a number of common decision problems, it is shown that simple models that visualise the results of the AM decision process in time are powerful tools to store the insights produced by reliability engineering tools in memory. Such understanding is required in deciding on maintenance strategies to be applied, as well as on achieving agreement and endorsement between/from the various parties involved, in order to guarantee a long-lasting success of an implementation and to evaluate the results with field data.

Even these simple models yield results that hitherto are surprising to practicing engineers, as demonstrated by their use in the long series of Master Course RAM blocks. It is our experience that, after graduation, most course members successfully apply these techniques in practice.

Keywords: Asset Management, Decision Support Techniques, Dealing With Uncertainty, Stochastic Analysis

List of abbreviations

AM	Asset Manager
CFO	Chief Financial Officer
CI	Critical Infrastructure
ETA	Event Tree Analysis
FMECA	Failure Mode Effect and Criticality Analysis
FTA	Fault Tree Analysis
HAZOP	HAZard and OPerability Study
MM	Maintenance Manager
NASA	National Aeronautics and Space Administration
RAS	Risk Assessment and Safety
RBD	Reliability Block Diagram
RCM	Reliability Centred Maintenance
SMART	Specific, Measurable, Achievable, Realistic, Time-bound
TPM	Total Productive Maintenance

1. Introduction

Vital services continuity is a major societal security issue in modern society. The supply of the vital services is guaranteed thanks to a large variety of Critical Infrastructures (CIs). Some CIs' disruptions may endanger the security of the citizen, the safety of the strategic assets and even governance stability. The ESReDA project group (CI-PR/MS&A-Data) focusses on Modelling, Simulation and Analysis of these complex, interconnected systems aiming at providing decision support to a wide range of stakeholders including (multi)national emergency management, critical infrastructure asset managers, policymakers, and the society.
The dependencies between such critical infrastructures are complex and frequently non-obvious. Examples as the electric power disruptions in California in 2001 demonstrate cross-sectoral cascading consequences with time-dependent failure characteristics and (positive) feedback of natural gas production, pipeline fuel supply, refinery and power production. Such consequences may in reliability engineering terms be typified as low probability events in complex systems with extensive consequences developing in time. Within that context the experience built up in reliability and risk assessment/asset management in simpler systems (like industrial production processes, water management and the built environment, where the probability of occurrence is one to two orders larger and consequences the same order lower), may provide lessons learned.

2. The History and Progress of Reliability Engineering

2.1 Where do we come from?

The 2nd World War created the need for new systems to be developed, manufactured and put into operation in a short time; the learning curve had to become steeper. The English radar installations in the Second World War necessarily employed while still in the development phase showed a mean time between failures in tropical conditions of a few hours. The Germans were quite unlucky with launching their first V-1 missiles to destroy London; research after the war estimated a 40% failure rate of air-launched V-1s.

> *On the German side, the failures met with launching the first V-1 missiles led Robert Lusser, a mathematically oriented aviation engineer to presage systems theory thinking by bringing in new concepts of system representation and random failure. He went beyond the deterministic way of thinking of skilled engineers and introduced rules for the reliability of systems as a function of those of the components. The "weakest link" paradigm was born; the reliability of a series system with statistically independent failure mechanisms equals the product of the reliabilities of the components. In hindsight, this observation appears rather obvious for anyone with even a limited insight in probability theory. However, it gives an intriguing insight into the deterministic engineering mindset at that time, being focussed on component design and apparently missing the system insight. Lusser himself was so convinced of his theories to get in a furious dispute with Wernher von Braun, who led a team to "put a man on the moon", declaring in 1947 openly [1]that "man can never go to the moon, let alone to Mars." To his insight, because of the complexity of the spacecraft required, there was simply too much chance to fail; "the probability odds with which he had wrestled a lifetime were simply too great for the risk". Lusser felt morally obliged to leave the design team, went back to Messerschmitt-Bölkow in Germany where he investigated the reliability aspects of the adaptations that the company was making to the F-104 Starfighter, the results of which soon turned out to be tragically correct. During a skiing holiday he ruptured his Achilles tendon and spent his last days and a lot of his personal fortune trying to market a ski binding he had designed to release stress just at the right time. He was 69 when he died in January of 1969, seven months before engineers succeeded in what he thought to be in reliability terms almost impossible; Neil Armstrong as the first human to set foot on the moon and to came back safely .*

This story, in a nutshell, exemplifies the problems we meet in the use of reliability engineering principles in Asset Management. The majority of asset managers have a mechanical, electrical or nautical engineering background. Engineers rely on the use of *"safety factors*[1]*":* the ratio of a structure's absolute strength (structural capability) to actual applied load; considered to be a measure of the reliability of a particular design. Typical values for building structural members are 2, for pressure vessels 3.5 to 4, aircraft and spacecraft use 1.2 to 3.0 depending on the application and materials. This approach, however, results in engineers mentally exclude the potential lack of reliability in operation; failures thus consequentially becoming regarded as "acts of God" or realisations of Murphy's Law.

> *These thoughts are in line with the attitude of NASA on using risk calculations in the Apollo project. The calculated expected mission success probability was that low that it discouraged [2] NASA from further quantitative risk studies until after the Challenger accident in 1986. Instead, NASA relied on FMECA stud-*

[1] A constant required value, imposed by law, standard, specification, contract or custom, to which a structure must conform or exceed. This can be referred to as a design factor, design factor of safety or required factor of safety. Typical values for building structural members are 2, for pressure vessels 3.5 to 4, aircraft and spacecraft use 1.2 to 3.0 depending on the application and materials.

ies and extensive testing; the risk study results were not widely circulated in NASA and sparingly if ever, released to the public at large. Literature shows many examples of situations where engineers met unexpected reliability/safety problems and searched for external support. Reliability Centred Maintenance was born after United Airlines suffered from severe reliability problems which could not be solved by making the overhaul periods shorter. They took the lead to define a generally applicable approach for the design of maintenance programmes, now known as the MSG-1 (maintenance steering group) documents. MSG-1 is the primitive forerunner of RCM (Reliability Centred Maintenance). MSG-1 was rooted in engineering insight and lacked most of the quantitative aspects. MSG-1 was followed up by later versions up to MSG-4. The ministry of Defence[[3] issued in 1975 a contract to United Airlines to describe this process. In 1978 Stanley Nowlan and Howard Heap [3] fulfilled this contract and published the landmark report "Reliability-Centred Maintenance". In line with the DoD requirements, they brought in quantitative aspects under the heading "actuarial analysis", using hired-in statisticians. Its rather misleading interpretation of (overall /sub-system, not a component or single failure mode!) failure mechanisms (**Fig. 2-1**) still remains in RCM textbooks and publications.

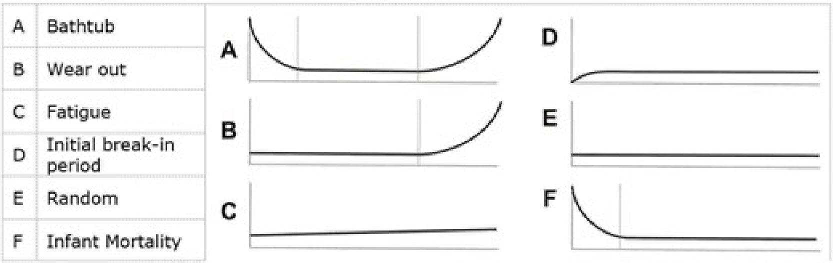


Fig. 1

Throughout history [4], the pendulum has been swinging back and forth from qualitative, experience (RCM, FMECA, HAZOP, TPM, ..) towards quantitative (ETA, FTA, RBD, ..) based decision support techniques. In cases where government bodies like the American Department of Defence or Industry experienced severe reliability problems, funding for academic research was widely available; technical problems were cast in stochastic OR research studies. However, most of the investigators had no direct link with real operations and considered the problems as interesting mathematical problems.

> *To quote Richard Barlow, one of the founders of reliability engineering [5]: "A mathematician is not going to read a typical engineering textbook because it is just too empirical."*

It is, therefore, no surprise that the mathematical models receive little interest in the engineering community [6] whereas properly used they proved to be capable to solve real industrial problems [7]. In 2009 the author published[8] the results of a survey under Dutch maintenance engineers showing that in spite of the significant economic consequences and problems with outsourcing contracts, the level of underpinning and monitoring failure data and maintenance strategies leaves to be desired. The EFNMS (European Federation of National Maintenance Societies) survey of 2011, [9] arrives at similar conclusions; safety and costs score higher than system output. In both surveys, engineers mainly use qualitative techniques where the chance aspects and time-dependent characteristics are easily neglected. Ultimo [10], a provider of Maintenance Management software, published in 2018 a report based on inputs from 150 MM's showing that MM's are rather focussed on technical aspects; only half of them having information on their contribution to the business. The repeated benchmarking studies from Solomon Associates [11] continue to observe apparent anomalies. From an engineering point of view differences in performance should logically be caused by such physical issues like size, age, location or organisational aspects like unionisation. However, in the long series of benchmarks [12] they continue to observe large variations in performance; the return on investment (ROI) varies from 16 per cent for the pacesetters to 4% in the bottom quartile plants. Unexpectedly, these differences show up for plants of the same ownership. The correlation with physical factors is quite weak; Solomon observes old plants both at the top as well as at the bottom of their ranking results and complexity plays a minor role. Such observations are in line with the results of the Merit team study in Shell [13].

In conclusion, over a period of some seven decades, we observe no large progress from experience towards evidence-based industrial asset (maintenance) management. The lack of systems theory, time-dependent behaviour and dealing with uncertainty in the education of engineers may be regarded as an impediment.

2.2 A comparison with control engineering

Management problems can well be compared to process control problems. It is the task of a process control engineer to keep the output of a process (or any other process variable) at the desired value (the set point) in spite of external disturbances and changes in process characteristics. To that end, the actual process output value is compared with the desired (set) value. Any deviation (Fig. 2-2*) between the two is translated by a controller into steering one or more control variables.*

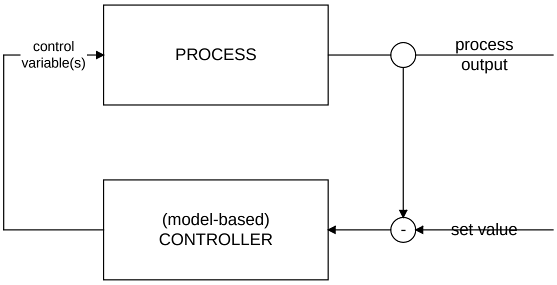


Fig. 2

Let us try to follow the reasoning of a control engineer. Before he/ she will start to work on a control problem the person will first check whether two conditions are met:

Observability: without mathematical rigour, this means that one can determine the full dynamic behaviour of the entire system from the system's outputs; you can write down the transfer function P from input to output. Controllability: again loosely speaking, this describes the ability of steering (control) inputs to move the internal state of a system from any initial state to any other final state in a finite time interval.

If one of these conditions is not fulfilled he/she knows that the control approach will fail.

Take the simple example of controlling your room temperature with a gas fired boiler. There is a temperature sensor in the room thermostat (observability) and the radiators receive hot water (controllability) from a boiler. First, think about the situation without feedback control; your thermostat is decoupled and the gas flow to the boiler is set at a certain value. The (room) temperature will then reach an equilibrium where the incoming heat supply Q_{in} just balances the heat loss Q_{out} =(area A * heat transfer coefficient U* temperature difference) = A *U* ($T-T_o$). We thus have, in simple lumped form, for the heat mass MC_p :

$$MC_p \frac{dT}{dt} = Q_{in} - UA(T - T_o)$$

$$\tau \frac{dT}{dt} = -T + ku$$

$$where$$

$$\tau = \frac{MC_p}{UA}$$

$$ku = \frac{Q_{in}}{UA} + T_o$$

If the gas flow rate is changed stepwise, the room temperature will reach exponentially a new equilibrium value:

$$T(t) = \left(1 - e^{-t/\tau}\right) ku$$

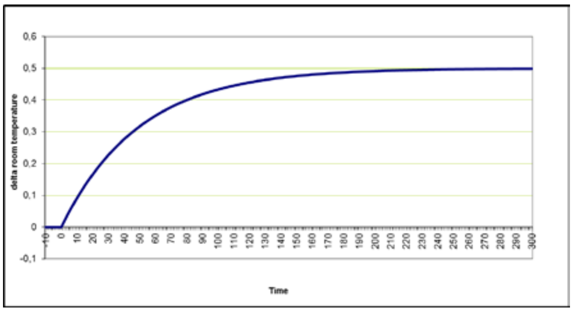


Fig. 2

An example is given in Fig. 3. This is the open loop response of the system; with no control present, the room temperature will decrease if the outside temperature drops. If we close the loop as in Fig. 3 the response with proportional control only will be (Fig. 4):

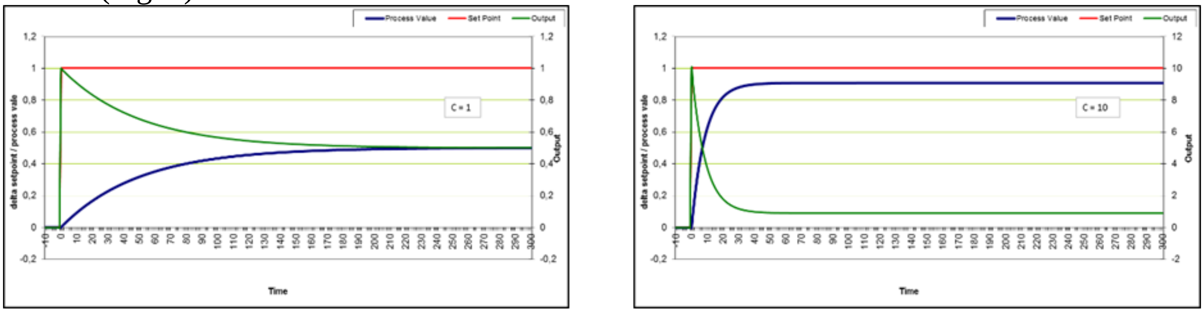


Fig. 3 Examples of closed loop control with various controller gains; P = 1

The deviation between set and measured value depends on the loop gain; the steady state error ε (measured value –set value) equals 1/ (1+PC) where P and C are the gains of the process (here 1) and controller, respectively. Time constants and external disturbances are reduced in the same proportion. Obviously, the control engineer aims at a minimum value of ε but now the dynamics of the system (amplitude and phase shift between set and measured value) play a role. First, we will make the model a bit more realistic:

- The gas flow to the burner will not increase immediately; again a first-order process (FOP).
- The temperature of the water spiral due to the increase in burning gas flow leads to another FOP.
- So, will the local temperature of the water.
- The now hotter water needs to flow from the boiler to the cv radiator; control engineers denote this as a “distance velocity lag” or “dead time”.
- The air in the room has to be heated up with the now hotter radiator.
- The temperature measurement will inevitably show (small) delay.

It can easily be shown that a series of exponential lags can be approximated by a dead time τ_d with a resulting phase shift $\omega\tau_d$. In the figure below we have extended the first order model with a time constant 100 of Fig. 4 with a dead time term with value 10.

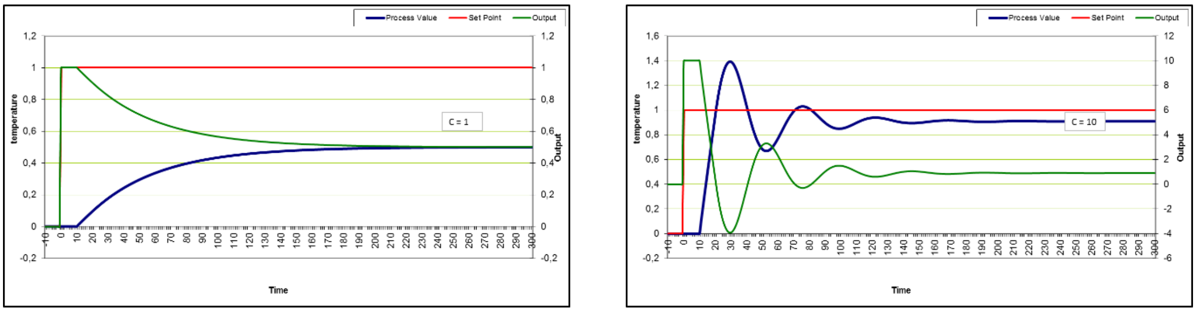


Fig. 4 The effect of a dead time on process stability

For the same controller gain setting of 10, we now observe significant oscillatory behaviour (Fig. 5). To understand this phenomenon we have to realise that both P and C are complex variables characterised by magnitude and phase shift. The transfer function reads H(s) = C(s) / (1 + P(s)C(s)) in the Laplace domain.

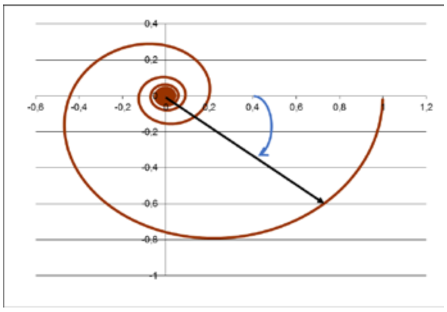


Fig. 5

Such a function may be sketched in the Nyquist diagram of Fig. 6 showing the magnitude (length of the vector) and phase angle of PC for increasing frequencies. Note that PC may approach the value -1 for a specific frequency where the gain tends to infinity. You may have experienced this phenomenon at a festival where the singer approaches with his microphone too close to the speakers!

With the transition from pneumatic to electronic controllers and later to full computer control the way towards more intelligent control was opened. In a number of cases, control variables may be strongly correlated, e.g. if you increase the temperature in a polypropylene solvent type reactor, the reaction rate increases consuming more pro-pylene whereupon the reactor pressure will automatically drop. Rosenbrock [14] de-veloped an engineering, *decoupling* approach to deal with this type of *multivariable* problems, using models based on transfer functions in the complex domain thus ena-bling the transition from single input – single output (SISO) to multiple input – mul-tiple output (MIMO) control loops. Later, mathematicians like Kalman [15] and Athans [16] developed the concept of linear, time-invariant multivariate optimal con-trol with models in state-space notation. From there on, model-based, nonlinear, mul-tivariable, adaptive and robust control theories were developed both in the frequency, as well as in state space domain. Pseudo-random binary sequence (PRBS) signals U(i,k) excite the system in such a way (Fig. 7) that the response Y(I,k) can be used to fit a model in state space or in the time domain without seriously affecting process throughput or product quality. The resulting black box model is valid in a small re-gion around the nominal process values only and the cause-consequence relationship is lacking. A more robust model is obtained if apriori information about the model structure and related physical processes is used in combination with the identification (a grey-box model).

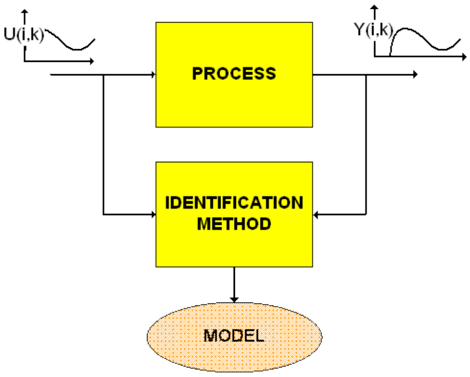


Fig. 6 Model identification in process control

The model-predictive approach was quickly taken up by Industry to stabilise and op-timise more complex systems, respectively optimisation objectives. Shell introduced Dynamic Matrix Control ([17]) already in the seventies These techniques now find their way, via vendors as AspenTech, Honeywell, Emerson, Rockwell Automation and others who offer complete model and software libraries. In all cases, optimal (production rate/envelope, energy, ...) operation is found either by white box models, correlations obtained by (on-line) system identification (black box) or a mix (grey box). If the model predictions start to deviate from actual behaviour, plant and labora-tory measurements are used to re-tune the model parameters. A distinct change from the analogue PID controllers is that digital model predictive control uses a control trajectory taking into account process constraints[2] such as maximum flow (pump ca-pacity), maximum cooling (duty of heat exchangers), vapour transport (compressor).

[2] In most cases optimality is found at operation at one or more constraints!

Modern process control is fully accepted in Industry at large. Whereas control engineering started as a specific, separate discipline with specialists groups active only in major plants of large companies, nowadays it is integrated into the curriculum of chemical/process engineers. Supported by instrumentation vendors, these chemical engineers are qualified to install both simple and complex control and optimisation loops.

3. Decision making in Asset Management

3.1 Introduction

To start with, in contrast with control engineers, measured information in maintenance management is scarce and of a stochastic, rather than deterministic, nature. Since designers aim, within the scope of the budget, at high reliability, the frequency of observed failures is low (MTTF for critical items ranging from 5 -15 years in Industry, 20 - 50 and more in civil). Reliability databases at best give a range of MTTF's mainly at equipment level, seldom at a specific failure mode level. The trending of condition data leaves to be desired; in statutory inspections, we observe that only the last results are stored by both parties as a "permit to operate" for the next period.

As a consequence maintenance engineers rely on "expert opinion" gathered in a series of team discussions where a basic system model and the few reliable data stored in the CMMS act as a framework for discussion. The well-known psychological traps as described by e.g. Kahneman and Tversky ([18]) like anchoring, scaling, bias due to availability, affect influenced, base rate fallacies, conjunction fallacies, ... require a well-skilled facilitator to steer the team and keep them motivated[3] through a number of meetings they are unfamiliar with and compete in time with their daily duties.

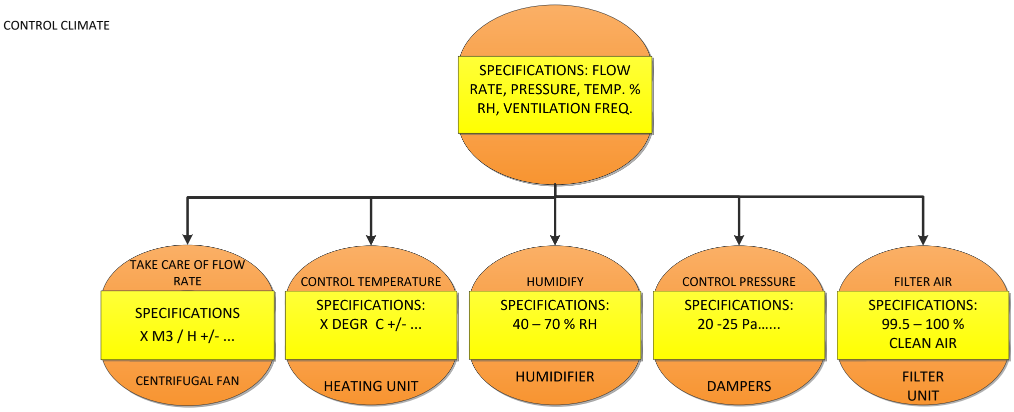

CONTROL CLIMATE
SPECIFICATIONS: FLOW RATE, PRESSURE, TEMP. % RH, VENTILATION FREQ.
TAKE CARE OF FLOW RATE
SPECIFICATIONS X M3 / H +/- ...
CENTRIFUGAL FAN
CONTROL TEMPERATURE
SPECIFICATIONS: X DEGR C +/- ...
HEATING UNIT
HUMIDIFY
SPECIFICATIONS: 40 – 70 % RH
HUMIDIFIER
CONTROL PRESSURE
SPECIFICATIONS: 20 -25 Pa......
DAMPERS
FILTER AIR
SPECIFICATIONS: 99.5 – 100 % CLEAN AIR
FILTER UNIT

Fig. 8

3.2 The toolbox of MM's

From various sources ([19-21] we know that the most frequently used decision support models in asset management are in descending order of frequency of use:

- Reliability Centred Maintenance (RCM)

[3] RCM is called mockingly Resource Consuming Monster!

- Failure Mode Effect (and Criticality) Analysis (FMECA) in combination with Risk Matrices.
- Reliability Block Diagrams (RBD)
- Fault / Event Tree Analysis (FTA, ETA)

All these techniques require a model of the process to be maintained (compare with the process control model discussed before). First of all, the asset register and the associated drawings have to be in place and updated. Functional block diagrams are recommended by IEC608012 and MIL_STD 1629A as a basis for FMECA and by Smith ([22]) as a basis for RCM. Zaal ([23]) uses the " hamburger model" (Fig. 8)

The question now arises how can these tools, in the light of the control engineering approach, support the asset manager in taking effective decisions:

- How do we make effective use of engineering knowledge and plant data to understand the system behaviour? (the control model)
- How can we substantiate the link between a maintenance procedure and the effect on the overall system requirements (the control action)
- How can a maintenance strategy be secured in the organisation (stability of control, observability of the desired trajectory in time)
- How do we make effective use of information to update the initially chosen strategy (the control feedback/ adaptation loop)

Aspect	RCM	FMECA /RM	FMECA/RP	RBD	FTA
Goal oriented' the line of sight"	☹	😐	😐☺	☺	☺
Mental model	☹	😐	😐☺	☺	☺
Lack of bias	☹	😐☺	☺	☺	☺
Completeness of model	☹	😐	😐	😐☺	☺
Need for field data	☺	😐☺	😐☺	☹	☹
Time dependent information	☹	☹	☹	☺	☹
Economic underpinning	☹	😐	😐☺	☺	n.a.
Acceptance in the organisation	☺	😐	😐☺	😐☺	😐☺

Table I

The asset manager requires the "line of sight"; how do his / her decisions influence the goals of the organisation? RCM focusses, in principle, on one specific failure mode and uses a broad description of the effects of failure: "trivial" versus "non-trivial" The FMECA approach conveys, for a list of functional failures, information on the ranges of likelihood and consequences. The RBD is the most complete system-modelling tool; it provides insight on the process layout and, depending on the level of detail employed, it presents quantitative information on the cost-benefit of either “bought in reliability” in the design phase (the MTTF specification in the purchase order) and that of maintenance strategies. The FTA is rather similar but now the line of sight is mainly on the functional availability of safeguarding components to prevent a critical top event; economics then does not play a strong role.

Most of these techniques rely on input from a panel of experts. A requirement then is that each member of the team has an identical mental model of the problem. RCM does not have inherent characteristics to fulfil this goal; facilitators need to discuss the problem in the group to ascertain a common understanding. In FMECA the panel members are required to fill in significant detail on each fm but the overall system characteristics are part of the panel discussion

The sloppier the method, the more a person in the team may be influenced (biased) by others assuming their skill/experience is better. This applies foremost for RCM; again the quantity of prescribed input in the FMECA approaches calls for a more structured common opinion. In principle, RBD’s and FT’s suffer least from bias since, preferably, they use factual data where possible and may analyse subjective opinions via sensitivity analysis.

Building an RBD or FT is a major exercise carried out by well-trained engineers. It is quite common to note that these models start with coarse process blocks (mostly from the P&ID) and refined / more detailed in subsequent stages. In this way, the completeness of the model can well be managed. RCM, on the other hand, allows engineers to pick out fm’s that have drawn attention because of system behaviour/insight “this component must be rather critical, because ….” or in root cause analysis “we now have to get rid of this recurrent problem”. The analysis thus easily can be stopped if the team decides that the most interesting fm’s are covered. FMECA stands in between; the primary list of fm’s for one system unit invites panel members to dis-cuss others to be added.

Field data are essential in a learning organisation but, in practice, are difficult to get. RCM suffers least from this aspect; on the other end of the spectrum designers of RBD’s / FT’s should realise that their quantitative results critically depend on the accuracy of the input data and sensitivity analyses thus are a must. FMECA stands in the middle; the method uses ranges rather than specific values.

In order to be effective (SMART), the results of decisions have to be monitored over time. The decisionmaker thus needs to have information on the expected time-dependent character of the eventual observations. RCM and FMECA lack this support, relying fully on long term averages. The logic background of RBD’s and FT’s allow in theory such a description in the time domain and RBD packages invariably show the decision maker what to expect in the future given his decision. Since FT’s are mainly used in safety/risk studies they commonly use point probabilities (long term averages) and thus produce point estimates of the probability of the undesired top event. Dynamic FT’s have been introduced to specifically model sequence of events for scenario analysis.

The CFO will require a cost-benefit analysis of the use of such decision support techniques. RCM is notoriously poor at this point, FMECA provides better estimates of the ranges to be expected but not on the timing. RBD’s are superior; not only do they clearly demonstrate the underlying mechanisms of economically rewarding asset management decisions (the causal link) but also the pattern how and the time horizon

it will take to become observable[4]. RBD's thus will give clear information to the final decision maker what and when to expect.
For a decision support tool to be effective, it should be fully accepted in the organisation. At that point, the simplicity of RCM is a plus. FMECA's are mainly used in well organised ISO 55001 compliant organisations. The more an organisation endorses this norm, the more FMECA will be an accepted tool. However, we also note that in public tenders the then required FMECA is regarded as an inevitable burden for which an outside consultant needs to be hired both for the process, as well as for the input data. It then is no surprise that the FMECA results will not easily become an effective improvement method. In most organisations, the construction of RBD's and FT's will be a dedicated task for in-house or external specialists. We then have the problem that the organisation is not well positioned to check the quality of this pro-cess and may take the results indiscriminately.

We have seen before that the success of process control and optimisation relies on insight in the ***possibilities*** *of control (controllability aspects, various types of control actions), in the* ***process*** *(the process model from black box to detailed process design or dynamic flowsheet type),* ***time-dependent behaviour*** *and* ***feedback*** *from* ***observed*** *data. From the list above we realise that in asset management the variety in maintenance strategies is limited, the underlying (deterioration) processes are poor understood, input (reliability) data are lacking to a great extent, decision support models frequently are aimed at long term averages only whereas on-line information on condition (and thus feedback) is scarce. A control engineer would classify such an approach as " open loop control" and warn for the consequences!*

4. Training Asset Managers; closing the gap between theory and practice

4.1 Introduction

We always start the Risk Assessment and Safety (RAS) Master course block by asking the participants what specific training will help them to build up their career. The majority responds along the lines of; "give us the tools to convince operational c.q. higher management that we take the best decisions possible"; that is more substantiat-ed decision making.
From the control engineering, perspective the (future) MM's then should:

- Realise that they deal with the realisations of inherently stochastic processes, the outcomes of which are furthermore strongly influenced by operational conditions.
- Only the total system contributes to the profitability of the company, hence the effect of a single failure mode should be translated to the effect at system level.
- The selection of a maintenance strategy (the control action) depends on the type of deterioration process (Weibull beta), the expected economic benefit and the maintainability aspects/quality of execution.

[4] Later on we will discuss that the observability of these improvements may be difficult, given the inherent stochastic nature of the failure processes where strong overlaps in probability distributions may take place.

- In order for the decision to be accepted by the organisation and properly assured over the lifetime of the process, the outcomes of the decision support tool need to be transparent; they should properly explain the results to be expected in time as well as the inherent variations.
- After implementation, the observed results should be compared with the decision model outcomes (the feedback loop). However, this loop is very slow due to the low frequency of occurrences of critical failure modes. Furthermore, the stochastic character requires correct statistical analysis. For high MTTF values, periodic observation of conditions is the only practical way to learn the effect of decisions.
- Given the usually restricted employment period of the decision maker in relation to the lifetime of the installation, significant attention has to be given to the necessary storage of data and underlying information.

All this requires at first a proper understanding and mental image of the inherent underlying uncertainties. All engineers in the past had some training in basic probability theory that will be refreshed in the Master RAS course but experience shows that they regard this as “mathematical exercises” like standard arithmetic’s that they solve along with the rules provided. A good starting point is the basic example of throwing a dice, students now that the chance of throwing a 3 is, as taught, on average 1/6 but do not realise that this holds only for a large number of repetitions. A simple Excel programme that shows how this probability develops over the series of throws (Fig. 9) effectively helps to memorise the stochastic behaviour; for most of the students, this is an aha experience!

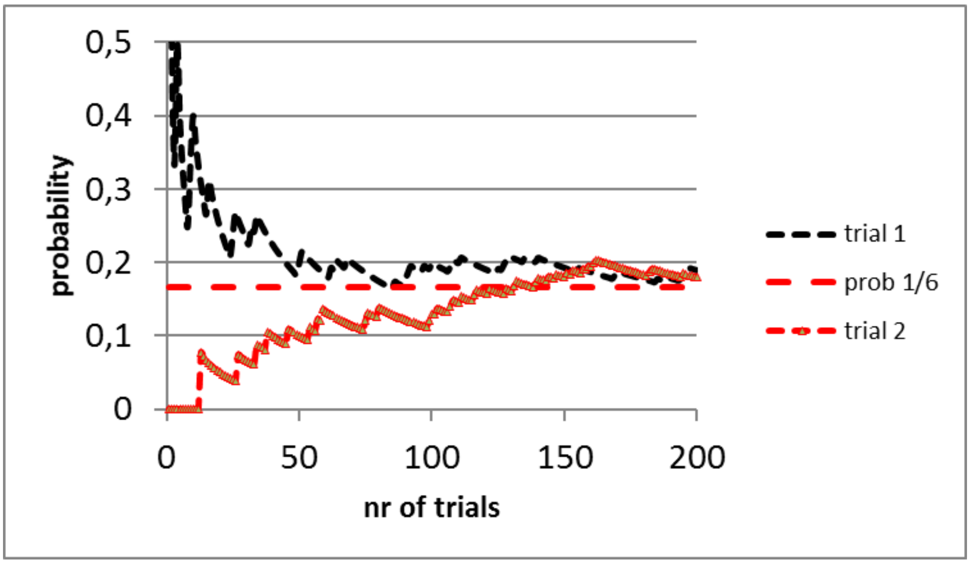
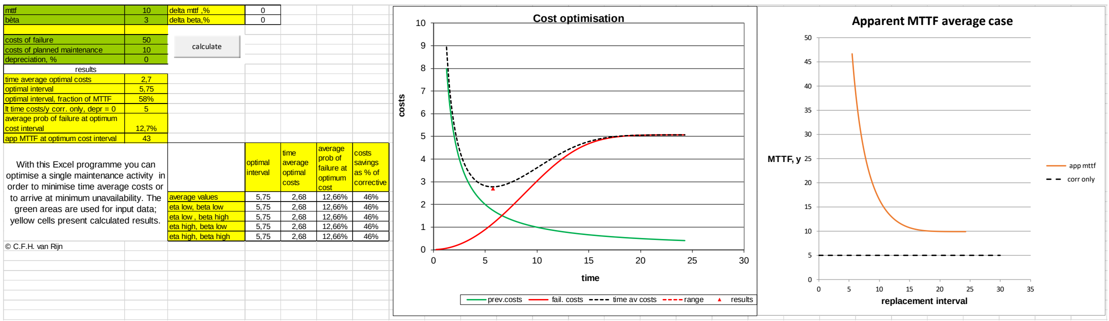


Fig. 9

4.2 Maintenance Management decision support tools

MM’s need to learn how to change from “gut-based” reasoning to the use of data and (Weibull) probability distributions. Regrettably, most organisations lack a proper failure database, especially over time periods that are sufficient to analyse. We strongly advise against the use of the, since the nineties obsolete [24], MIL-HDBK-217 figures and inform that important partners have left the OREDA organisation. So, we challenge them, to use the “expert opinions” of in-house specialists in a structured team approach, paying specific attention to differences in individual opinions that unexpectedly may cast light on failure patterns. A general observation is that these engineers misinterpret the MTTF as a kind of useful life or guarantee period; to their surprise discovering that at that specific moment in time roughly 2/3 have failed! Combining individual 10, 50, 90 % estimates on the time to failure followed by visualisation of the expected failure pattern in time, the team arrives at (a range of) reasonable estimates of the Weibull scale and shape parameters, now trusting that, if used in computer models, the outcomes are in line with the best, substantiated opinion availa-ble, but sensitivity analyses are needed.



mttf	10	delta mttf ,%	0
bèta	3	delta beta,%	0
costs of failure	50	calculate	
costs of planned maintenance	10		
depreciation, %	0		
results			
time average optimal costs	2,7		
optimal interval	5,75		
optimal interval, fraction of MTTF	58%		
lt time costs/y corr. only, depr = 0	5		
average prob of failure at optimum cost interval	12,7%		
app MTTF at optimum cost interval	43		

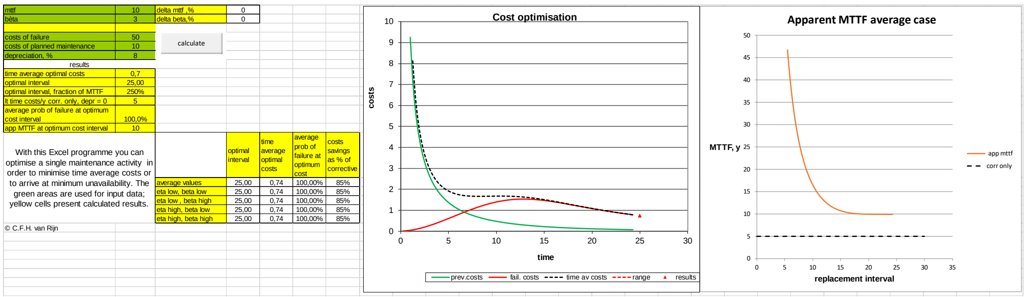
With this Excel programme you can optimise a single maintenance activity in order to minimise time average costs or to arrive at minimum unavailability. The green areas are used for input data; yellow cells present calculated results.

	optimal interval	time average optimal costs	average prob of failure at optimum cost	costs savings as % of corrective
average values	5,75	2,68	12,66%	46%
eta low, beta low	5,75	2,68	12,66%	46%
eta low , beta high	5,75	2,68	12,66%	46%
eta high, beta low	5,75	2,68	12,66%	46%
eta high, beta high	5,75	2,68	12,66%	46%

© C.F.H. van Rijn

Fig. 10

Such data may be used in the selection and optimisation of time-based planned maintenance with the Barlow-Proschan model of Fig. 4-2. In this case, the failure mode has an MTTF of 10 years with a beta of 3 and the cost ratio between planned and corrective maintenance is 5. If the costs are booked on the operational budget without discounting, the model calculates an optimum replacement interval of 5.8 years where the time average PM costs are 46% of the corrective costs. It also shows that at this point one may expect about 13% of the failures under a corrective strategy leading to an apparent MTTF of 43 years. Compared with an RCM study, the MM now gets a view on the economic consequences. The apparent MTTF plays a role in the criticality matrix of an FMECA; to what extent reduces PM the failure frequency compared with corrective only?



mttf	10	delta mttf ,%	0
bèta	3	delta beta,%	0
costs of failure	50	calculate	
costs of planned maintenance	10		
depreciation, %	8		
results			
time average optimal costs	0,7		
optimal interval	25,00		
optimal interval, fraction of MTTF	250%		
lt time costs/y corr. only, depr = 0	5		
average prob of failure at optimum cost interval	100,0%		
app MTTF at optimum cost interval	10		

With this Excel programme you can optimise a single maintenance activity in order to minimise time average costs or to arrive at minimum unavailability. The green areas are used for input data; yellow cells present calculated results.

	optimal interval	time average optimal costs	average prob of failure at optimum cost	costs savings as % of corrective
average values	25,00	0,74	100,00%	85%
eta low, beta low	25,00	0,74	100,00%	85%
eta low , beta high	25,00	0,74	100,00%	85%
eta high, beta low	25,00	0,74	100,00%	85%
eta high, beta high	25,00	0,74	100,00%	85%

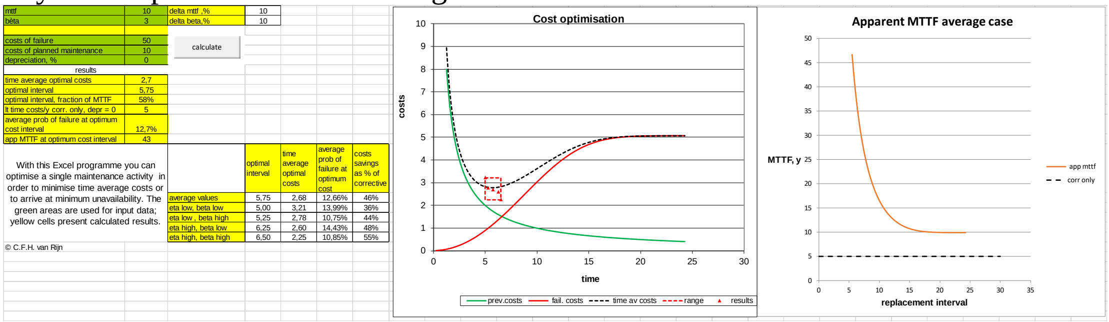
© C.F.H. van Rijn

Fig. 11

However, if the costs of replacement are such that the CFO regards this as a capital investment, the discounting percentage[5] plays a strong role (Fig. 11). If the MM has to use a discounting percentage of 8% the optimum is lost; the model advises not to

[5] Note that this DCF is one of the major instruments of a CFO to rank investments and has virtually no relation with the sometimes stated comparison with receiving interest from a bank or the average yield in the stock market!

perform PM. This information may be used to change the opinion of the CFO to classify such replacements under the general investments.



mttf	10	delta mttf ,%	10
bèta	3	delta beta,%	10
costs of failure	50	calculate	
costs of planned maintenance	10		
depreciation, %	0		
results			
time average optimal costs	2,7		
optimal interval	5,75		
optimal interval, fraction of MTTF	58%		
lt time costs/y corr. only, depr = 0	5		
average prob of failure at optimum cost interval	12,7%		
app MTTF at optimum cost interval	43		

With this Excel programme you can optimise a single maintenance activity in order to minimise time average costs or to arrive at minimum unavailability. The green areas are used for input data; yellow cells present calculated results.

	optimal interval	time average optimal costs	average prob of failure at optimum cost	costs savings as % of corrective
average values	5,75	2,68	12,66%	46%
eta low, beta low	5,00	3,21	13,99%	36%
eta low , beta high	5,25	2,78	10,75%	44%
eta high, beta low	6,25	2,60	14,43%	48%
eta high, beta high	6,50	2,25	10,85%	55%

© C.F.H. van Rijn

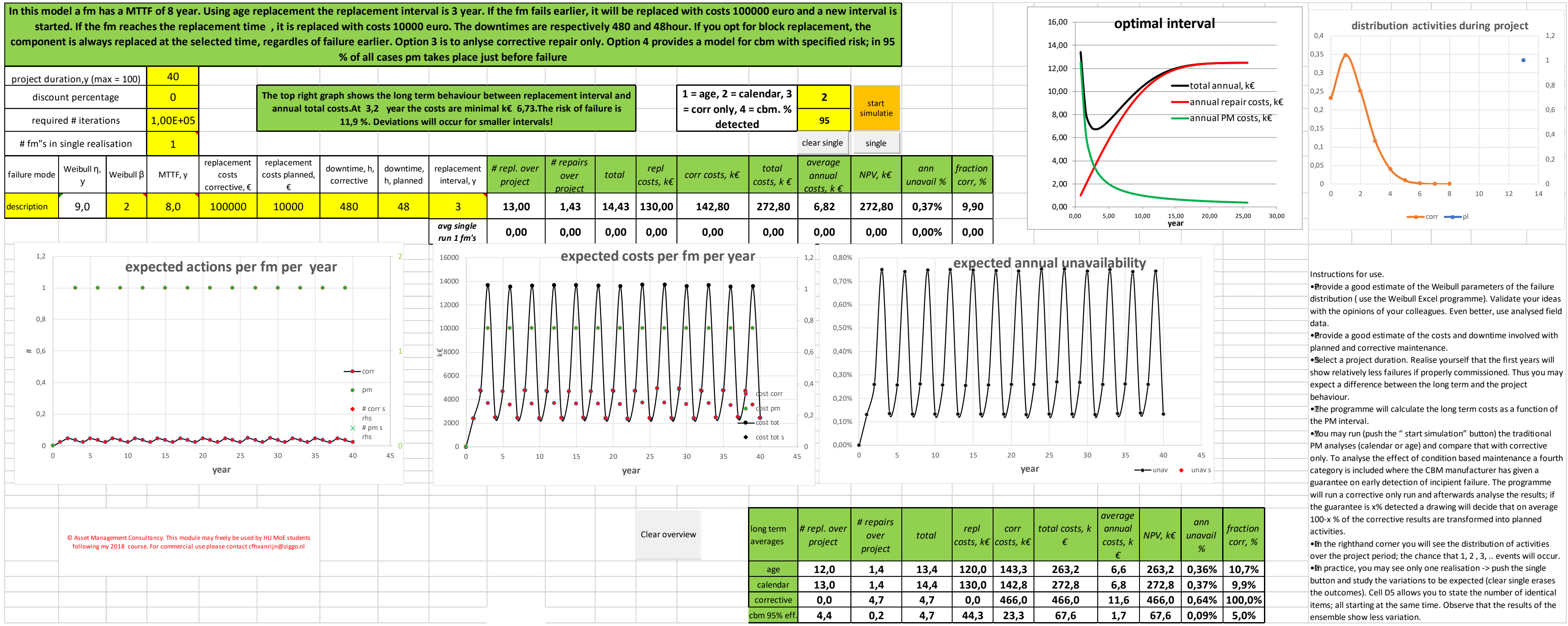
Fig. 12

The CFO may also be critical on the expected economic benefit. A sensitivity analysis where a range of +/- 10% in the Weibull parameters is used shows that the expected savings range between 36 and 55%. The MM now also realises that the optimum replacement interval at best can be estimated to lie between 5 and 6.5 years. This range aspect is never used in the timing of work orders in the CMMS; exactly after, in this case, 5.8 years the CMMS will generate a work order. If the PM is not executed, the CMMS will increasingly remind the MM of the backlog in PM's executed. Since this is regarded as a key performance indicator, this message will eventually reach higher management and the MM will critically be questioned.

This is a nice example of Goodhart's Law[6]*: "When a measure becomes a metric, it ceases to be a good measure"; in other words, when we set one specific goal, people will tend to optimize for that objective regardless of the consequences. The management objective, in this case, is to reduce the frequency of failures, which subsequentially should be monitored in time, but instead, the PM action required is followed. I have seen occasions where MM's hired in extra, even less skilled, mechanics to keep this KPI at level, disregarding costs and quality of execution!*

Unfortunately, long term averages have a specific meaning only at the design level where equipment selection and various configurations are investigated. Operations are faced with performance in specific time periods; with a Design, Build, Finance and Maintain contract (DBFM), the contractor is responsible for the design and construction of the project, as well as for financing and total maintenance over a specified time period. Furthermore, the employment period of most MM's is short in comparison with the slow dynamics of critical, thus with large MTTF values, failure modes. Hence, the MM needs a quick analysis / "what if tool" to get a perspective on the realisation in time. A simple Monte Carlo analysis then is of great help (Fig. 13).

[6] More precisely: "any observed statistical regularity will tend to collapse once pressure is placed upon it for control purposes."



In this model a fm has a MTTF of 8 year. Using age replacement the replacement interval is 3 year. If the fm fails earlier, it will be replaced with costs 100000 euro and a new interval is started. If the fm reaches the replacement time , it is replaced with costs 10000 euro. The downtimes are respectively 480 and 48hour. If you opt for block replacement, the component is always replaced at the selected time, regardles of failure earlier. Option 3 is to anlyse corrective repair only. Option 4 provides a model for cbm with specified risk; in 95 % of all cases pm takes place just before failure

project duration,y (max = 100)	40
discount percentage	0
required # iterations	1,00E+05
# fm"s in single realisation	1

The top right graph shows the long term behaviour between replacement interval and annual total costs.At 3,2 year the costs are minimal k€ 6,73.The risk of failure is 11,9 %. Deviations will occur for smaller intervals!

1 = age, 2 = calendar, 3 = corr only, 4 = cbm. % detected	2
	95

failure mode	Weibull η, y	Weibull β	MTTF, y	replacement costs corrective, €	replacement costs planned, €	downtime, h, corrective	downtime, h, planned	replacement interval, y	*# repl. over project*	*# repairs over project*	*total*	*repl costs, k€*	*corr costs, k€*	*total costs, k €*	*average annual costs, k €*	*NPV, k€*	*ann unavail %*	*fraction corr, %*
description	9,0	2	8,0	100000	10000	480	48	3	**13,00**	**1,43**	**14,43**	**130,00**	**142,80**	**272,80**	**6,82**	**272,80**	**0,37%**	**9,90**
								avg single run 1 fm's	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00**	**0,00%**	**0,00**

Instructions for use.

- Provide a good estimate of the Weibull parameters of the failure distribution (use the Weibull Excel programme). Validate your ideas with the opinions of your colleagues. Even better, use analysed field data.
- Provide a good estimate of the costs and downtime involved with planned and corrective maintenance.
- Select a project duration. Realise yourself that the first years will show relatively less failures if properly commissioned. Thus you may expect a difference between the long term and the project behaviour.
- The programme will calculate the long term costs as a function of the PM interval.
- You may run (push the “ start simulation” button) the traditional PM analyses (calendar or age) and compare that with corrective only. To analyse the effect of condition based maintenance a fourth category is included where the CBM manufacturer has given a guarantee on early detection of incipient failure. The programme will run a corrective only run and afterwards analyse the results; if the guarantee is x% detected a drawing will decide that on average 100-x % of the corrective results are transformed into planned activities.
- In the righthand corner you will see the distribution of activities over the project period; the chance that 1, 2 , 3, .. events will occur.
- In practice, you may see only one realisation -> push the single button and study the variations to be expected (clear single erases the outcomes). Cell D5 allows you to state the number of identical items; all starting at the same time. Observe that the results of the ensemble show less variation.

long term averages	*# repl. over project*	*# repairs over project*	*total*	*repl costs, k€*	*corr costs, k€*	*total costs, k €*	*average annual costs, k €*	*NPV, k€*	*ann unavail %*	*fraction corr, %*
age	**12,0**	**1,4**	**13,4**	**120,0**	**143,3**	**263,2**	**6,6**	**263,2**	**0,36%**	**10,7%**
calendar	**13,0**	**1,4**	**14,4**	**130,0**	**142,8**	**272,8**	**6,8**	**272,8**	**0,37%**	**9,9%**
corrective	**0,0**	**4,7**	**4,7**	**0,0**	**466,0**	**466,0**	**11,6**	**466,0**	**0,64%**	**100,0%**
cbm 95% eff.	**4,4**	**0,2**	**4,7**	**44,3**	**23,3**	**67,6**	**1,7**	**67,6**	**0,09%**	**5,0%**

Fig. 13

In the right hand upper corner, the MM finds the long-term optimisation[7] similar to that in Fig. 10. This optimal interval is used in a time-dependent analysis with data in the yellow cells. He/she may select five different maintenance strategies:

- Corrective repair, run to failure; repair takes place after failure.
- Calendar based optimisation; a strategy where we replace at fixed calendar intervals and in-between apply corrective maintenance (to an "as good as new" condition) whenever a failure occurs. We assume that this replacement will always take place at the planned moment, even if the element had to be correctively repaired just before.
- Age replacement; a maintainable element is replaced or restored to "as good as new" when it reaches a specific age t_p. If it fails before t_p we will apply corrective maintenance leading to the same situation as with PM. From that moment on, we start counting the t_p interval again. As such, it has a serious drawback on the scheduling of planned maintenance actions. Every time we encounter a failure within a predetermined PM interval we start a new cycle.

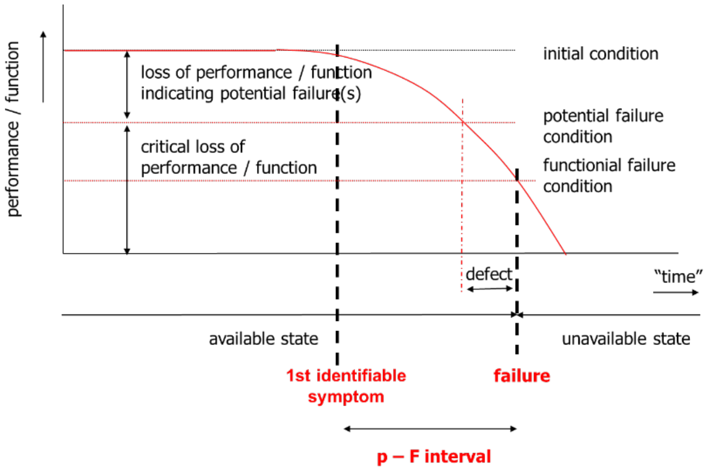
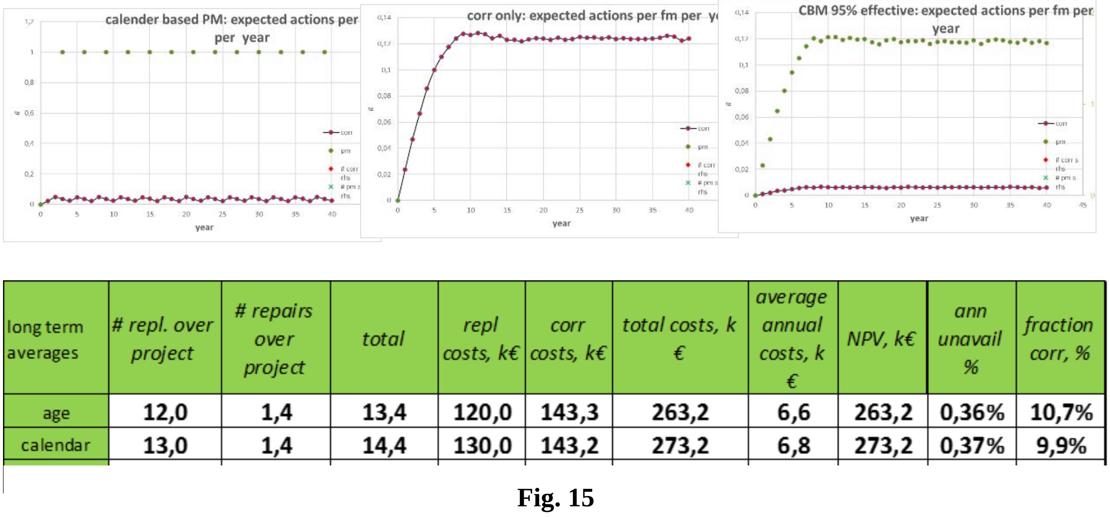


Fig. 14

- Using the PF interval (Fig. 14); a deceptively simple idea promoted by John Moubray [25] as a rather strange mix-up of a deterministic treatment of inherently stochastic processes since both the occurrence of the first identifiable symptom and the interval between this value and the loss of function (failure) will show acceptable spread in practice and thus should be treated as stochastic processes. Furthermore, we note a mix-up of concepts on a measurable condition (say, a wall thickness) and a probability of functional failure; the relationship of which is frequently difficult to determine. Professor Anthony Christer [26, 27] later on developed the concept of the delay time model which overcomes part of these restrictions but uses the stationary behaviour to find optimal solutions, for instance on the inspection interval given a probabilistic description of the occurrence of P and the P-F interval.

[7] For reasons of clarity, we have left out here the required sensitivity analysis on the input parameters!

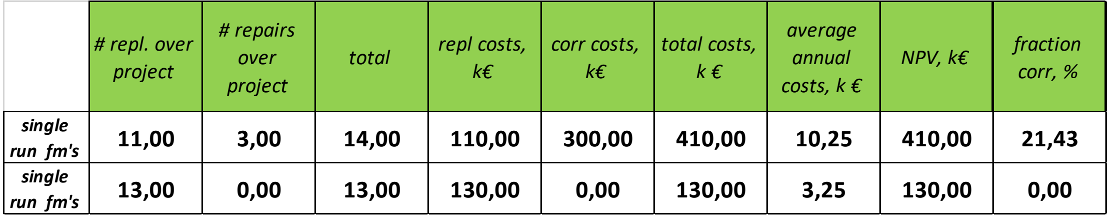
- Using condition based maintenance; in this case, specifying only the degree of effectiveness, that is the percentage of imminent failures detected by the CBM system that early, that corrective repair could effectively take place. Note that the MM should primarily be interested in this result, rather than the techniques behind the CBM technique.



long term averages	# repl. over project	# repairs over project	total	repl costs, k€	corr costs, k€	total costs, k €	average annual costs, k €	NPV, k€	ann unavail %	fraction corr, %
age	12,0	1,4	13,4	120,0	143,3	263,2	6,6	263,2	0,36%	10,7%
calendar	13,0	1,4	14,4	130,0	143,2	273,2	6,8	273,2	0,37%	9,9%

Fig. 15

With this tool, the MM easily gets insight into the average time-dependent behaviour of the various measures of control (the maintenance strategies) and their cost-effectiveness (Fig. 15). In the top-right corner, he/she will notice the pdf of the corrective / PM activities to be expected. For instance, if the calendar based PM strategy is chosen, 13 replacements will need to be executed but, in spite of the PM action, on average 1.4 failures needing corrective action are expected with 23% probability of zero, up to a 5% probability of 4. It is the experience of the author, however, that this graph does not directly lead to a mental impression that is easily memorised. For that purpose, the MM may opt for a series of single runs of the MC simulation of (Fig. 13) making the pdf clear to him/her (Fig. 16).



	# repl. over project	# repairs over project	total	repl costs, k€	corr costs, k€	total costs, k €	average annual costs, k €	NPV, k€	fraction corr, %
single run fm's	11,00	3,00	14,00	110,00	300,00	410,00	10,25	410,00	21,43
single run fm's	13,00	0,00	13,00	130,00	0,00	130,00	3,25	130,00	0,00

Fig. 16

All CMMS system will detect patterns of successive failures with unexpected small time intervals in between. This raises concern in the organisation, potentially leading to a more specific investigation like a root cause study. The MM should realise, however, that such series of events are inherent characteristics, albeit with small probability, of a stochastic process!

There is a strong trend nowadays towards the use of condition-based maintenance, predictive maintenance and exploiting the “Industrial Internet of Things, IIoT” where data cheaply and easily become available towards the revolution of “Industry 4.0”.

Again, this forms a fruitful area for mathematical research, but a word of caution is on its place.

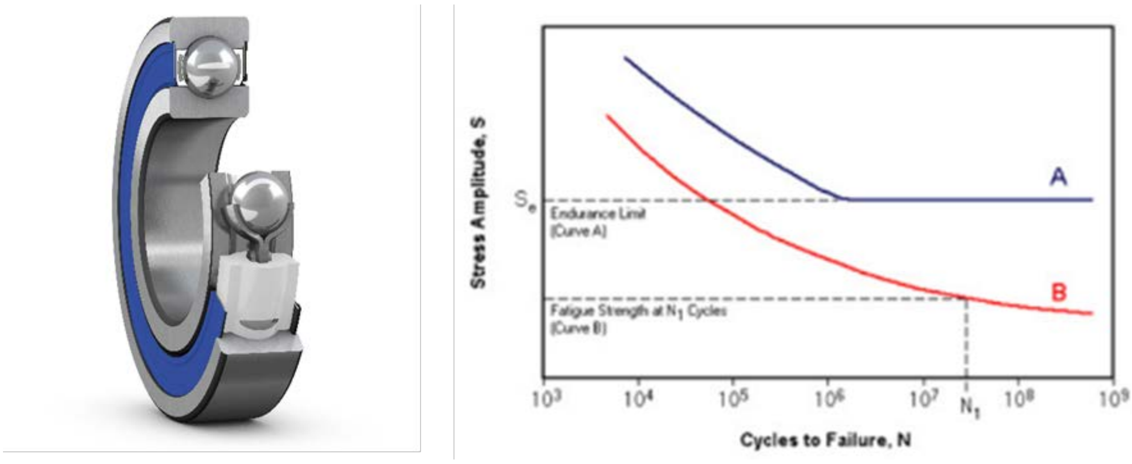


Fig. 17

Bearings (roller, ball, Fig. 17) are indispensable components of rotating equipment, failure of which causing appreciable downtime, costs and frequently loss of production. In theory (and in design) bearing life is determined by the number of hours/cycles it will take for the metal to "fatigue" which is a function (SN curve) of the load on the bearing, the number of rotations, and the amount of lubrication that the bearing receives. Hardened steel (curve A) shows a fatigue limit (or endurance limit); a value of the stress below which a material can presumably endure an infinite number of stress cycles which is the basis of the Lieblein- Zeelen [28] design equation. In practice, bearing life is limited and shows large variations (e.g.Van Rensselaer [29], Zaretsky [30]) with low Weibull beta values (around 1.5). There is a common understanding that the, in theory, infinite lifetime ends by external causes (misalignment, vibration, shock, dirt, corrosion pitting, excessive heat) causing operation outside the fatigue limit and subsequentially rapid deterioration.

Bearing health is monitored by vibration measurements. A simple vibration alarm may indicate the point of onset of deterioration (comparable with the “point” P in the PF interval). From that moment, the modelling of failure, the predictive approach, becomes cumbersome. Jardine [31], in his extensive survey article, describes a large number of techniques: short-time Fourier transform, wavelet transform, proportional hazards models, hidden Markov models, independent component analysis, cluster analysis, AI techniques, artificial neural networks, fuzzy logic, belief networks, ...The fact that that many techniques are investigated is strongly linked with the lack of a proper deterioration model; the first particle of bearing steel or debris causes an avalanche of further deterioration in a rather random fashion, strongly influenced by operational conditions. The validity of the approach than may be questioned; what is the decision problem of the AM? If he/she accepts the warning signal (damage initiation has been confirmed), the fundamental decision problem lies with the grace period until this vibration increases to the shutdown level; is that period long enough to take proper action? Now we have a model to steer on along the philosophy of the PF interval as described above.

The IIoT is heralded as cheaply bringing in large amounts of data. However, the crux lies with the translation of these data into information for decision support, the dynamic model of degradation. Many techniques rely on observed correlations, but the causality remains unaddressed; a critical perspective is required!

4.3 Using process control models for CBM

As outlined above, process control engineers need to model the constraints of operation in order to optimise production. These constraints are usually found as maximum cooling rate, maximum gas flow, etcetera.

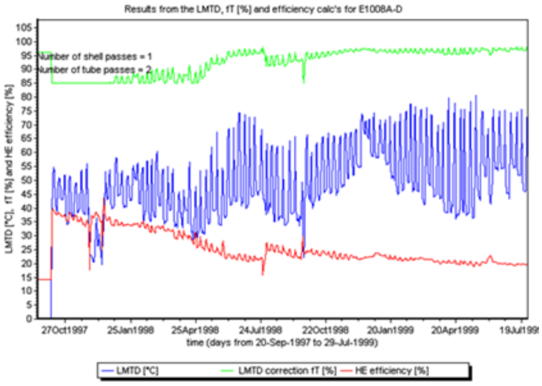
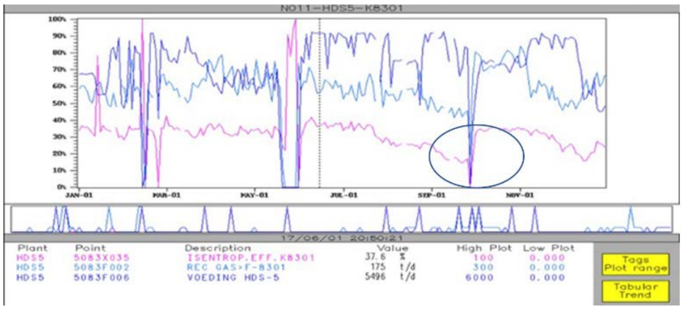


Fig. 18

Fig. 18 provides an example where the heat efficiency of a shell and tube heat exchanger is estimated from the flowrates and the logarithmic mean temperature differ-ence (the red curve). This concept was introduced in Shell by my research group in the eighties and now receives great attention; Chevron[8], using wireless transmitters and Microsoft's Azure cloud computing, expects "Savings could be in the millions if you can monitor and predict the health across all of our exchangers".



Plant	Point	Description	Value		High Plot	Low Plot
HDS5	5083X035	ISENTROP.EFF.K8301	37.6	%	100	0.000
HDS5	5083F002	REC GAS>F-8301	175	t/d	300	0.000
HDS5	5083F006	VOEDING HDS-5	5496	t/d	6000	0.000

Fig. 19

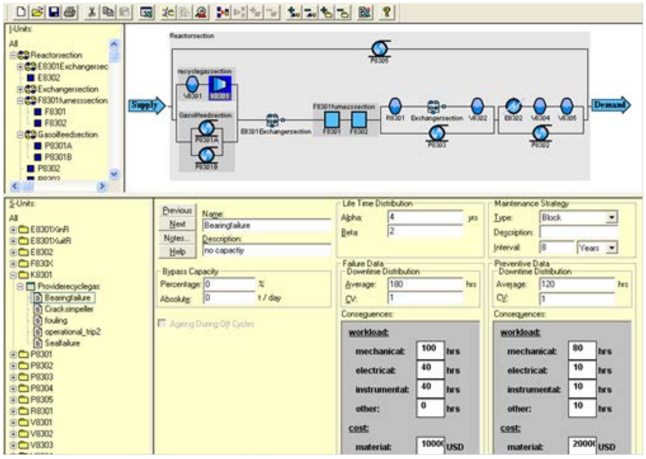
A similar concept can be followed to optimise the clean out rotary vane compressors (Fig. 19), note the effect of the cleanout operation in September. For pumps, the condition is assessed by following the relationship between the pump head centrifugal and the volumetric flow rate (Q), that a pump can maintain. Note that, in these cases, we use process measurements that frequently will already be available. Secondly, the model outcomes will readily be accepted by engineers, the

[8] https://blogs.wsj.com/cio/2018/09/05/chevron-launching-predictive-maintenance-to-oil-fields-refineries retrieved December 2018

more so, since they directly may be associated with production losses. Crossing the traditional cultural barrier between Operations and Maintenance thus has great value.

4.4 Maintenance Management decision support tools at system level

The simple tools described above produce results only at failure mode level, whereas the economic benefit is produced at the system level.



Name: Bearingfailure
Description: no capactiy

Bypass Capacity
Percentage: 0 %
Absolute: 0 t / day

Life Time Distribution
Alpha: 4 yrs
Beta: 2

Maintenance Strategy
Type: Block
Description:
Interval: 8 Years

Failure Data
Downtime Distribution
Average: 180 hrs
CV: 1
Consequences:
workload:
mechanical: 100 hrs
electrical: 40 hrs
instrumental: 40 hrs
other: 0 hrs
cost:
material: 1000(USD

Preventive Data
Downtime Distribution
Average: 120 hrs
CV: 1
Consequences:
workload:
mechanical: 80 hrs
electrical: 10 hrs
instrumental: 10 hrs
other: 10 hrs
cost:
material: 2000(USD

Fig. 20

Any master course will therefore treat the concepts of reliability block diagrams and fault trees. These calculations can either be calculated analytically (SPARC, Fig. 20) [32] or via Monte Carlo simulation (RAPTOR (free download), commercial software packages like BlockSim, AvSim, Maros, RiskTec, Miriam, ...). One of the authors of SPARC (now solely an in-house tool in Shell) has developed an interesting package called ARTIS (Availability and Reliability Tracking Information System) [9] for addressing the risks to production availability which includes event tracking from a CMMS.

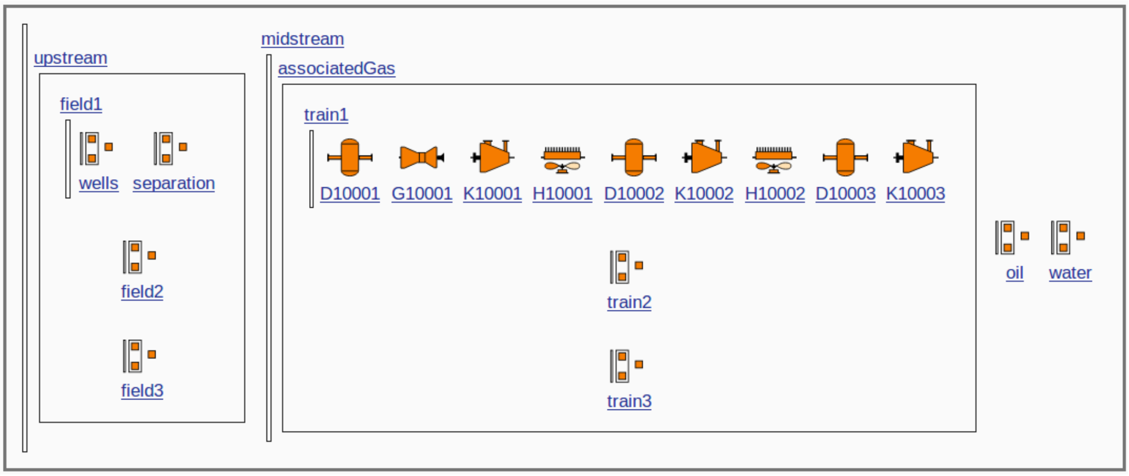


Fig. 21

[9] The user interface can be found at: www.artis.la/V24/models/artis.html, the user manual at wiki.artis.la

Artis is freely available for testing and demonstration purposes, small models can be run free of charge but, in this free mode, response times might be slow. Short- and long term service agreements are available for commercial use.

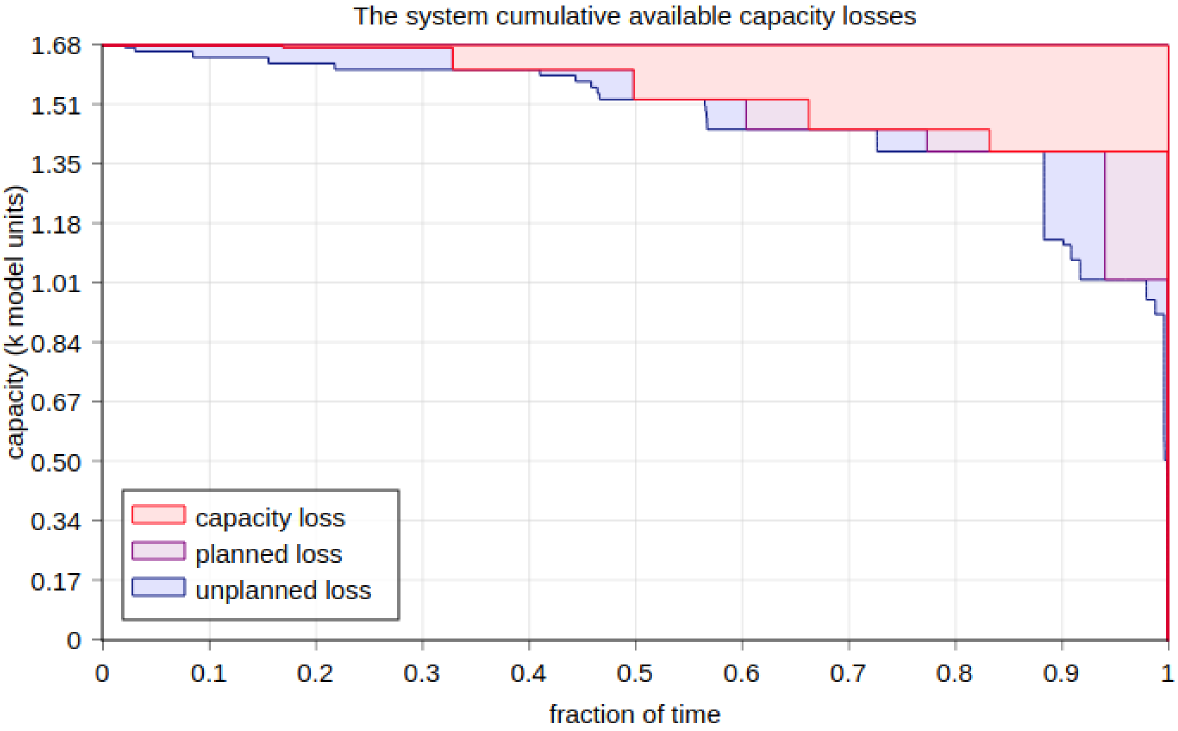


Fig. 22

This important system information can only be obtained if detailed information is available on the failure distribution and the maintenance data. In practice, the problem lies with the former; real data are available only after analysing data over a long period. For design purposes, where the problem frequently is to select alternatives of configurations, information from databases like OREDA [33] can be used with care. Fig. 22 gives an example of the capacity profile calculated with ARTIS of a gas production platform, where, using OREDA data, the initial configuration of 3 trains each with 35% capacity proved to yield insufficient system capacity, because of the train downtime. The design team proposed a fourth train but ARTIS showed that 3 trains each with 50% capacity were an economically better alternative.

For the optimisation of operational asset management, we are frequently forced to use engineering judgement, next to sparsely available data. Inevitably, there thus will be appreciable uncertainty of the quantitative (system) results which need to be investigated by sensitivity[10] analyses. The benefit of applying RBD packages then depends strongly on fast, but structured, "what if" analyses steering the team in reaching a good decision, rather than on achieving precise quantitative output values.

[10] Both SPARC and Artis allow the user to change all or a selected group of Weibull parameters by a chosen percentage for such an analysis.

4.5 Decision support in change programmes

Active asset managers regularly organise improvement procedures along the lines of "the number of unforeseen failures per month must be lower"; a valuable KPI. The change manager will formulate such a case in terms of:

- Setting a new performance goal.
- Investigating the expected reasons for a lower than desired performance.
- Ranking causes of failures, thus determining focus.
- Providing a clear distinction between and prioritization of controllable and non-controllable aspects.
- Clarity about the relationship between improvement measures and system performance.
- Controlled management of the implementation of improvement measures.
- Prognosis of effect improvement measures; how to validate the costs involved against the benefits expected?
- A managerial formulation of the way to monitor the progress of the improvement process in time.

Note the similarity with the process control approach! The last bullet item touches upon the observability of the maintenance process; remember that this is one of the pre-requirements of the control engineer but he/she is dealing with deterministic val-ues (measurements) rather than the outcome of stochastic processes like in mainte-nance. The asset manager may choose to monitor:

1. The process of improvement as observed by the estimated increase of the MTTF, which requires statistical investigation of the TTF of field data
2. The process of improvement as observed by the decrease in number of failures per time interval, which is the standard form of reporting in CMMS’s

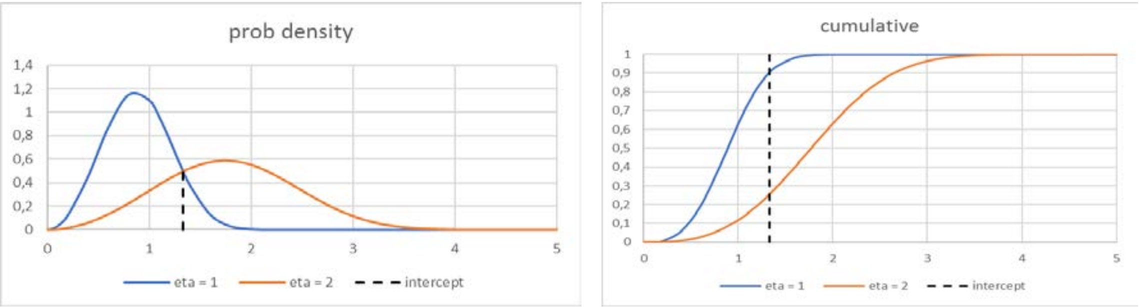


Fig. 23

Suppose, we have an improvement process in which the MTTF is doubled by choosing higher quality components (the scale factor eta of a Weibull distribution with shape factor beta 3 goes from 1 to 2). The left side of Fig. 23 shows the two probability density curves. The "measurement" (compare with process control) of our process now follows from drawing samples from the probability density distribution. However, we see that the two curves show an overlap that can be calculated from the cumulative distributions of process 1 and 2 (right side Fig. 23). We arrive at a value of 35%, which means that if we completely replace process 1 with process 2 we run a risk of 35% of drawing samples (observing failure) in the overlapping part. In those cases, we will not observe any improvement while it has indeed taken place! Hence, the observability is restricted to 65%.

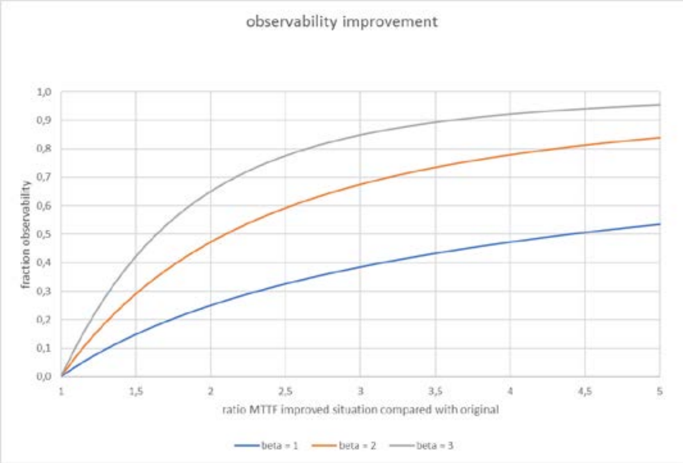


Fig. 24

Fig. 24 shows an overview in which the x-axis represents the ratio between the improved situation with respect to the original value and the y-axis the fraction of observability. Suppose that in practice we achieve an improvement of a factor of 2, we see that at a beta value of 3 (close to the normal distribution) we have a probability of approximately 65% to observe this improvement from the field data.) For completely random failure (β = 1) the probability drops to around 25%.

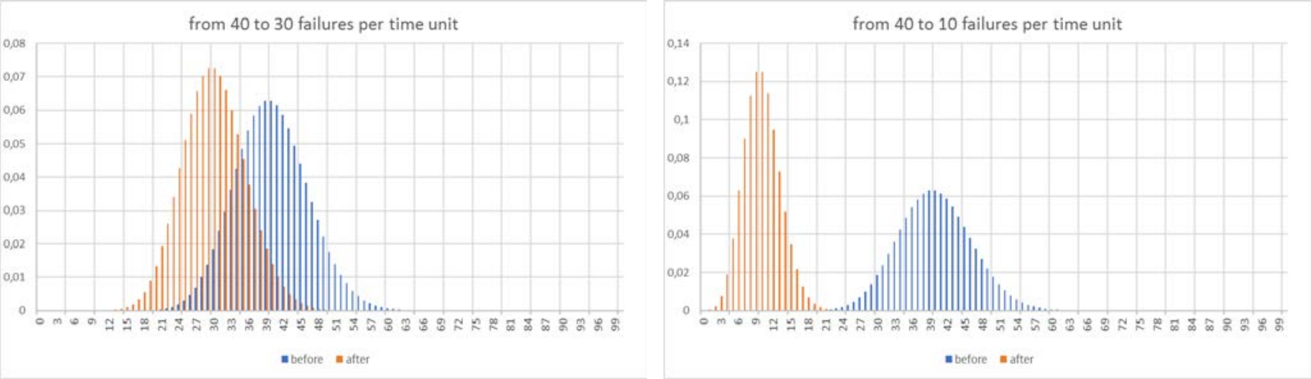


Fig. 25

Now, if the MM follows the number of failures in a given time period, we deal with a (for β > 1: pseudo) Poisson process. In such an improvement process as in Fig. 25 where the number of failures is reduced from 40 to 30 per period, we note again an overlap between the probability densities as can be seen in the left graph. This overlap becomes smaller as the achieved improvement increases; the right-hand graph shows that if the # of failures are reduced by 80%, the overlap almost disappears. If the observations lie in the common area of the two probability density functions we cannot make a distinction between the two situations; a change is unobservable.

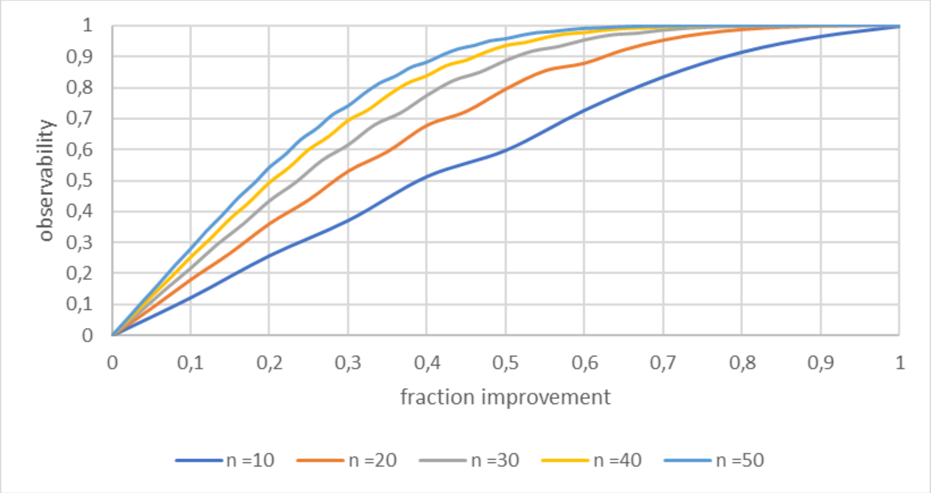


Fig. 26

Whereas the observability is 60% in the first case, it is 99,8% in the last one. The observability depends in this case (Fig. 26) on the number of failures in a time period *and* the fraction improvement. In the case of a relatively small improvement, we have to average over a very long interval.

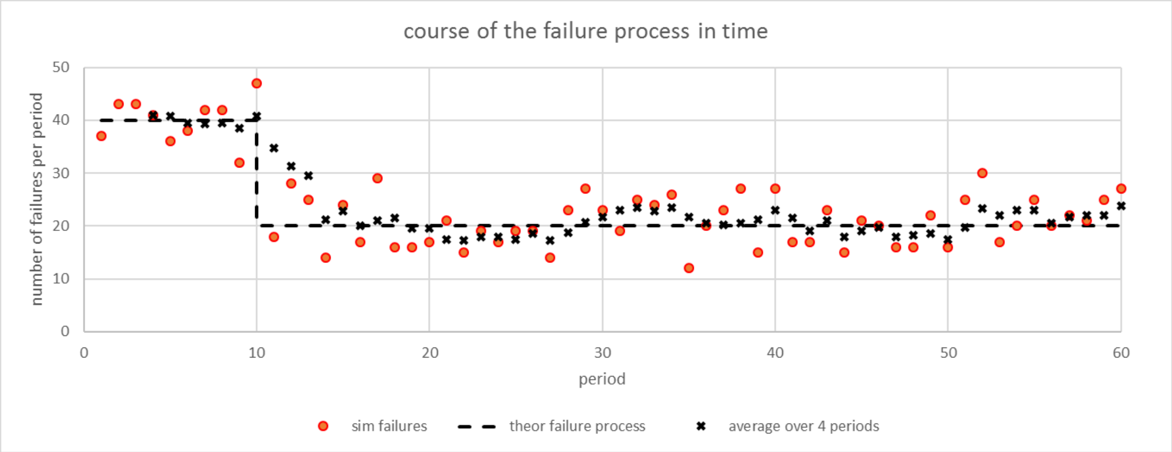


Fig. 27

Fig. 27 shows a simulation of a process with 40 components each having the same failure mode of the beta =1 type. At period 10 all 40 are replaced[11] by new compo-

[11] Such a sudden change is unrealistic in practice; the simulation model has a facility to take the implementation period in consideration but this facility is not used here for clarity.

nents with twice higher MTTF; reducing the expected number of failures per period from 40 to 20. The orange dots indicate the observed number of failures resulting from the simulation process; note the difference in each period between the expected and observed value. The black crosses indicate the rolling 4-period average; clearly a lagging indicator. In this process the observability is 94%; the improvement is noticeable after period 15.

Realise that Fig. 27 is just one realisation of this chance process; we may also observe a result as sketched in Fig. 9; where the asset manager may unjustified worry about the sudden increase in the number of failures between period 30 and 40.

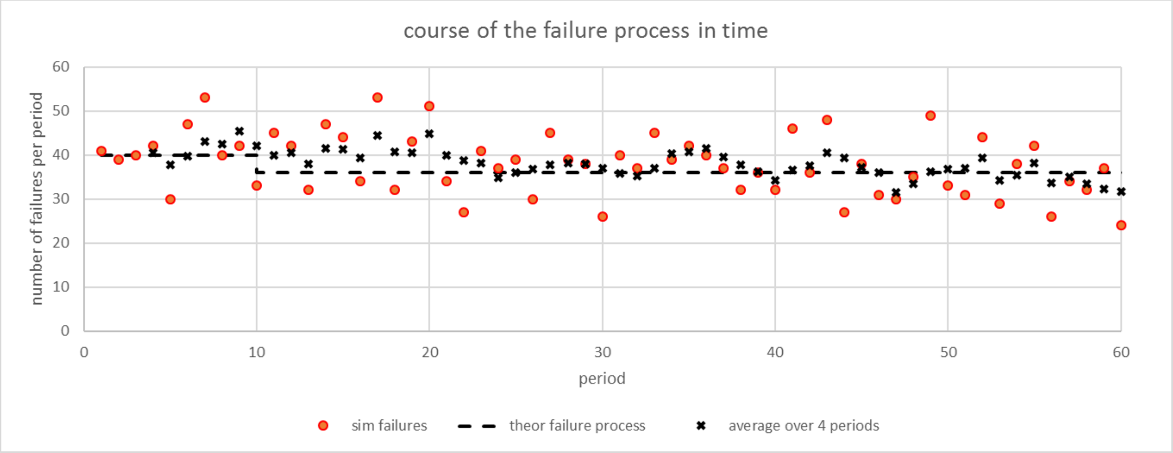


Fig. 28

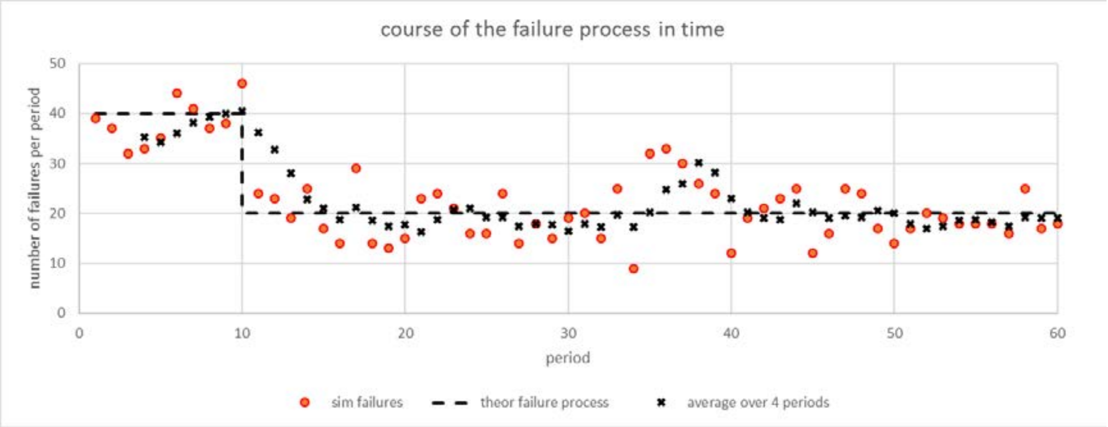


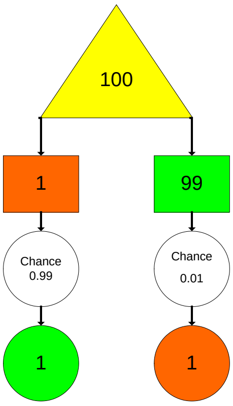
Fig. 29

In Fig. 29, the same process is sketched but now with an improvement of 10 %. The observability is here some 25% and in this specific realisation, the improvement is difficult to observe in the first 15 periods after the change.

4.6 Inspection

Statutory inspections with a regular return interval, both on the safeguarding aspects as well as on the physical condition, are a significant part of the Asset Management portfolio in complying with standards. One would, therefore, expect that results of these inspections over the lifetime of systems are readily available. However, in practice, frequently only the last results are stored / easily retrievable. In such cases, there is no trending and the information gathered thus does not contribute to a learning organisation.

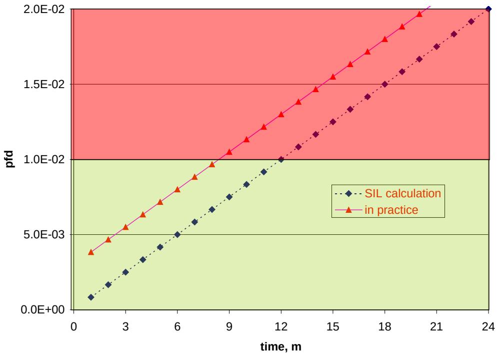
In safeguarding inspections, in line with IEC 61508, 61511, Bayes rule plays an important role, the type I type II error. The influence of human errors is clearly mentioned in the norms and even more detailed in application papers like [34], but in qualitative terms only. Since most engineers shy away from mathematics, the psychological approach of Gigerenzer [35] is effective.



Take the case where the required probability of failure on demand (PFD) is 10^{-2}. Gigerenzer warns that even an explanation in terms of percentages is psychologically less transparent than using pure numbers. Hence, he proposes the following approach: *"Assume that you have to test this item 100 times. To the best of our knowledge, we know that only in 1 out of these 100 cases there will be a defect. So, the fact that you repeatedly observe a functioning system is normal.*

I take it for granted, that you, as an experienced mechanic, say in 99 out of the 100 cases will correctly find this defect, repair it, such that it is working again.

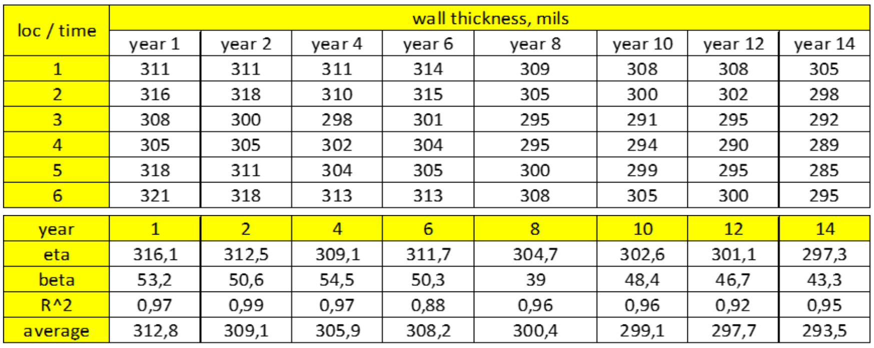
The problem now lies with the 99 cases where the component is functioning correctly. If you are not careful enough, you may introduce a fault; for instance, forget to put back the override switch. Suppose that this happens in 1 out of 100 cases, you see that testing does not improve the situation!



$$PFD = \frac{1}{2} * \lambda * T_i + p_{mi}$$

Fig. 30

Fig. 30 shows the formal results with λ the overall constant failure rate, T_i the inspection interval and p_{mi} the probability of maintenance induced failure. For the latter no formal data are available but students invariably estimate a range between 1 – 5 %. Accepting the views of Gigerenzer, from thereon they will better take care to guard the quality of intervention, for instance by using the "four eyes "principle.



loc / time	wall thickness, mils							
	year 1	year 2	year 4	year 6	year 8	year 10	year 12	year 14
1	311	311	311	314	309	308	308	305
2	316	318	310	315	305	300	302	298
3	308	300	298	301	295	291	295	292
4	305	305	302	304	295	294	290	289
5	318	311	304	305	300	299	295	285
6	321	318	313	313	308	305	300	295

year	1	2	4	6	8	10	12	14
eta	316,1	312,5	309,1	311,7	304,7	302,6	301,1	297,3
beta	53,2	50,6	54,5	50,3	39	48,4	46,7	43,3
R^2	0,97	0,99	0,97	0,88	0,96	0,96	0,92	0,95
average	312,8	309,1	305,9	308,2	300,4	299,1	297,7	293,5

Table II

Table II shows published data [36] on pipe wall thickness over a period of 14 years measured at 6 fixed locations with the fitted Weibull distributions. Note that the fit expressed by the R^2 value in year 6 and 12 is below 0.95; the 6 (!) data points showing appreciable scatter. The decrease in time of the beta values indicate the corrosion process to become more inhomogeneous

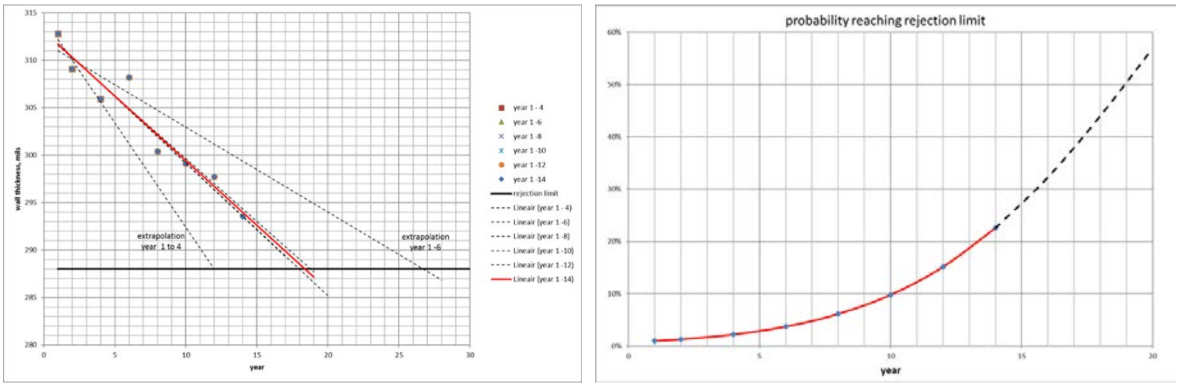


Fig. 31

The left side of Fig. 31 shows the trend of the decrease in wall thickness over time-based on the Weibull average value, which is comparable to that of the arithmetic averages of the measurements. Note the large uncertainty in extrapolated values over the first 6 years, gradually the expected time value of meeting the rejection limit stabilises around 18 – 19 years. The right side of Fig. 31 shows that the probability of crossing the rejection limit (the failure) steeply increases with time. Whilst the trending of the averages focusses the asset manager on the year of occurrence of passing the rejection limit (18 – 19 years), this figure shows that already in year 10 the risk is some 10%. Such information may be used in an economic evaluation of the optimal time of replacement, balancing the costs of early execution against that of operating below the rejection limit.

Field data are extremely valuable [37] [38] in a learning organisation. However, this requires the CMMS to be set up such that information at failure mode level becomes available whereas these systems usually focus at equipment level. The need to interpret textual information generated by technicians who are not trained on later use of the information at maintenance execution level is cumbersome.

5. Conclusions

Over the past seven decades, several benchmarking studies show that the effectiveness of Asset Management has not significantly changed; it appears that extensive academic research has not found widespread application.

We have shown that this evolution is at strong variance with that in the (comparable) discipline of control engineering. Process control is at the end of the learning curve and taught in standard curricula. Process engineers thus are professionally capable to use all kinds of measured/inferred process variables to set up stable simple and advanced control and optimisation systems, that are fully accepted in operation and of which the economic benefit is readily demonstrated.

In Asset Management most (especially, mechanical) engineers are technically driven and reason mainly in deterministic terms. Compared with control engineers, their system insight, views on observability and controllability and interest for time-dependent processes are less developed. Reliability engineering still is mainly an add on in engineering education; companies may at best have a few in-house reliability engineering specialists. These persons struggle with the lack of input data for decision support models and lack proper information on the physics / chemistry of degradation models. In monitoring the effect of implemented decisions, they meet a paucity of data. Thus, where applied, their decision support models do not easily find widespread support from colleagues and management. These models, aiming at long term characteristics clash with the drive for business results to be achieved in specific (in comparison with the system dynamics, short) time slots and the needs of a learning organisation.

Many academia in stochastic OR focus, frequently underestimating the data problem, on black box (statistical time to failure) develop decision support models aiming at long term averages; physics of failure only recently being partly included. It appears that the academic focus more lies on mathematically elegant solutions with novel techniques than on AM decision making in practice.

Discussing a number of common decision problems, we have shown that simple models that *visualise* the AM decision process in time are powerful tools to store the insights produced by reliability engineering tools in memory. Such understanding is effective in deciding on achieving agreement and endorsement between/from the various parties involved. With this insight, the inherent variability in realisations (observability) and the restrictions in management effectiveness (controllability) becomes part of the mental image. Structured team consultation provides suitable starting data at least for ranking and evaluating decisions; sensitivity analyses are necessary to provide an understanding of the spread in model outcomes. The uncertainty in input data should then, where possible, later on, be verified by processing field data.

Even these simple models yield results that are hitherto surprising to practicing engineers, as demonstrated by their use in a long series of Master Course RAM blocks. It is our experience that, after graduation, most course members successfully apply these techniques in practice.

References

1. Reid Collins. *Lusser's Law*. 2003 [cited 2018 23 april]; Available from: https://spectator.org/51313_lussers-law/.
2. Fragola, J.R. *Risk Management in US Manned Spacecraft: From Apollo to Alpha and Beyond*. in *Product Assurance Symposium and Software Product Assurance Workshop*. 1996. Noordwijk: European Space Agency.
3. Nowlan, F.S. and H.F. Heap, *Reliability-Centred Maintenance*. 1978, Office of Assistent Secretary of Defense: Washington CD 20301. p. 476.
4. van Rijn, C.F.H., *Current Status of Asset Management*, in *Reliability and Maintainability Impact to Asset management stakeholders; A practical guide for Asset Owners". An ESReDA Project Group Report*. 2014, Det Norske Veritas.
5. Block, H.W., *A Conversation with Richard Barlow*. Statistical Science 2001. **16**(4).
6. Dekker, R., A. Smit, and C.F.H. Van Rijn, *Mathematical models for the optimisation and their application in practice.* Maintenance, 1994. **9**(3): p. 22-26.
7. R.Dekker and C.v. Rijn. *PROMPT, A decision support system for opportunity-based preventive maintenance*. in *Reliability and Maintenance of Complex Systems*. 1987. ASI series F: Computer and Systems Sciences.
8. Van Rijn, C.F.H., *The status of Asset Management in a number of Dutch industries and service companies.*, in *37th ESReDA Seminar on Asset Optimisation and Maintainability*. 2009: Baden, Switzerland.
9. van Rijn, C.F.H., F. Magalhaes Neves, and M. Raza, *The Future of Asset Management; How do We Prove its Importance and Effectiveness?*, in *Reliability and Maintainability Impact to Asset management stakeholders; A practical guide for Asset Owners". An ESReDA Project Group Report.*, M. Raza, Editor. 2014, Det Norske Veritas.
10. Ultimo Software Solutions Ltd, *Trend Report Maintenance Manager of the Future*. 2018: Manchester.
11. L.H.Solomon. *Reduction of breakdown through productive maintenance*. in *Production Control in the Process Industry*. 1989. Osaka / Kariya Japan: Pergamon Press.
12. Bloch, H.P. and M. Hernu, *Performance Benchmarking Update: Expectations and Reality*. Maintenance & Asset Management, 2008. **23**(1): p. 34 - 38.
13. Narayan, V., J.W.Wardhaugh, and M.C.Das, *100 Years in Maintenance and Reliability; Practical lessons from three lifetimes at Process Plants*. 2007, New York: Industrial Press, Inc.
14. Rosenbrock, H.H., *Design of multivariable control systems using inverse Nyquist Array*. Proc. IEE, 1969. **116**: p. 1929-1936.
15. Kalman, R.E., *A new approach to linear filtering and prediction problems.* Journal of Basic Engineering, 1960. **82**(1): p. 35-45.
16. Athans, M., *Stochastic Robustness of Linear-Time-Invariant Control Systems.* IEEE Trans. Automatic Control, 1971. **36**(1): p. 82-87.
17. Cutler, C.R. and R.B. L.. *Dynamic matrix control—a computer control algorithm.* , in *AIChE 86th National Meeting 1979*. Houston,TX.
18. Tversky, A. and D. Kahneman, *Judgment under Uncertainty: Heuristics and Biases.* Science, 1974. **185**(4157): p. 1124-1131.

19. Van Rijn, C.F.H., *The status of Asset Management in a number of Dutch Industries and Service Companies*, in *37th ESReDA Seminar on Asset Optimisation and Maintainability*. 2009: Baden, Switzerland.
20. Komonen, K., *An overview on Strategic Physical Asset Management*, in *Reliability and Maintainability Impact to Asset management stakeholders. A practical guide for Asset Owners*, M. Raza, Editor. 2014, Det Norske Veritas.
21. IAM, *Asset Management - an Anatomy*. 2015, The Institute of Asset Management: London.
22. Smith, A.M., *Reliability-centered Maintenance*. 1993: McGraw-Hill.
23. Zaal, T.M.E., *Profit-Driven Maintenance for Physical Assets*, ed. S. Newton. 2011, Geldermalsen: Maj Engineering Publishing.
24. De francesco, E., R. De Francesco, and E. Petritoli, *Obsolescence of the MIL-HDBK-217: A critical review*, in *2017 IEEE International Workshop on Metrology for AeroSpace* 2017, AESS: Padua, Italy. p. 282-286.
25. Moubray, J., *Reliability Centred Maintenance II*. 2001, New York: Industrial Press Inc.
26. A.H.Christer , W.M.W., *Delay time models of industrial inspection problems.* Journal of Operational Research, 1984. **35**(5): p. 401-406.
27. A.H.Christer, *Modeling Inspection Policies for Building Maintenance.* J.Op.Res.Soc., 1976. **33**.
28. Lieblein, J. and M. Zelen, *Statistical Investigation of the Fatigue Life of Deep-Groove Ball Bearings.* Journal of Research of the National Bureau of Standards, 1956. **57**(5): p. 273 - 318.
29. Van Rensselar, J., *Tribological Bearing Testing.* Tribology & Lubrication Technology, 2014(April).
30. Zaretsky, E.V., *Rolling Bearing Life Prediction, Theory, and Application*, N.L.R. Center, Editor. 2016: Hampton, VA 23681-2199.
31. Jardine, A.K.S., D. Lin, and D. Banjevic, *A review on machinery diagnostics and prognostics implementing condition-based maintenance.*, in *Mechanical Systems and Signal Processing*. 2006. p. 1483–1510.
32. Smit, A.C.J.M., C.F.H. Van Rijn, and S.G. Vanneste, *SPARC: a Comprehensive Reliability Engineering Tool*, in *6th ESReDA seminar on: Maintenance and system effectiveness*,, J.Flamm, Editor. 1994, Joint Research Centre, Ispra, Italy: Chamonix-France.
33. SINTEF, *Offshore and Onshore Reliability Data 6th Edition, Volume 1 – Topside Equipment, Volume 2 – Subsea Equipment* 2015, Oslo: Oreda.
34. Anon, *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry*. 2001, OLF.
35. Gigerenzer, G., *Reckoning with risk*. 2002, London: Penguin Books.
36. Paul Barringer, H., *Pipe Wall Thickness Decisions Using Weibull Analysis*. 2019.
37. Van Rijn, C.F.H., *Maintenance Modelling and Applications; lessons learned* . in *32nd ESReDA Seminar Maintenance Modelling*. 2007, ESReDA: Sardinia, Italy.
38. van Rijn, C.F.H., et al., *Evidence-based, mission-oriented Corporate Real Estate Management*, in *46th ESReDA Seminar on Reliability Assessment and Life Cycle Analysis of Structures and Infrastructures*. 2014: Torino, Italy.

Probabilistic Models and Methods for Processing Data in "Smart" Monitoring System to Define Rational Preventive Measures of Supporting Reliability and Safety

Andrey Kostogryzov
Federal Research Center "Computer Science and Control" of the Russian Academy of Sciences (FRC CSC RAS), Vavilova Street 44, bld. 2, 119333 Moscow, Russia
and Main Research Scientific and Probatory Center of Robotics at the Ministry of Defense of Russian Federation, Seregina Street, 5, 125167 Moscow, Russia

Vladimir Artemyev, Jury Rudenko
Joint-Stock Company "Siberian Coal Energy Company - SUEK",
Dubininskaja Street, 53, bld. 7, 115054 Moscow, Russia

Oleg Kurpatov
Close Joint-Stock Company "Russian Telecom Equipment Company - RTEC",
Tverskaja Street 20, bld. 1, 125009 Moscow, Russia

Andrey Nistratov
The Russian Power Agency of Ministry for the Power Generating Industry,
Shepkina Street 40, bld. 1, 129110 Moscow, Russia

George Nistratov
The Research Institute of Applied Mathematics and Certification,
Krasnobogatyrskaja Street 2, bld.2, 17564 Moscow, Russia

Abstract

The approach to define rational preventive measures of supporting reliability and safety for modern critical systems is proposed. The approach is based on the original probabilistic models and methods for processing data in "smart" monitoring system, presented as "Black Box" and as complex structure. The models and methods are applicable in real time and also for short- and long-term planning. To define rational preventive measures of supporting reliability and safety 5 steps of the approach are described and demonstrated by practical examples.

Keywords: efficiency, method, model, probability, risk, system, technology.

1. Introduction

The digital transformation of modern critical systems requires a cardinal turn to rational preventive measures of reliability and safety provision on the base of data monitored. Here critical systems are understood as objects of dangerous manufacture and the equipment, energy objects, power and transport systems etc. Implementation of scientifically proved rational preventive measures to support reliability and safety on the base of probabilistic modelling and risks predictions helps to transform data gathering into "smart" system of monitoring. Different monitored data about current conditions of parameters become accessible in real time. A monitoring of parameters conditions is intended to increase reliability and industrial safety and to improve health management of critical systems and their operation efficiency. Analysis of actual data allows to be traced the losses of established norm ranges for various parameters and helps to define the reasons of abnormalities in time.

As the main metric only a frequency of failures is quite often used. It means exponential probability distribution function (PDF) of time before failures without details of different performed processes and conditions. Such simplified approach leads to deviations in a probability of failures which may be hundreds and thousands percent against the results of more adequate modelling [1]. Sometimes regression models are used for an analysis of expected changes depending on system operating time. For complex systems, integrated from subsystems and the elements of different destination, the regression estimations don't represent analytical dependences on concrete parameters and consequently don't allow to predict "bottlenecks" and to solve the inverse problems connected with optimization. But the analytical benefit, extracted from gathered data, is far from exhausted. More exact predictions are connected with creation the PDF of time before expected failures. For example, for analysed serial and parallel structures analytical approaches of PDF composition are developed [2-5], formulas describing probability density function for cascading disruption are proposed [6]. And also differential equations and simulation models are used, see for example [6-8 etc.].

Along with it «smart» monitoring systems differ that they should analyse gathered data considering high structural complexity of system, analytical dependences on the changes of concrete parameters, characterizing reliability and safety, on the used technologies of integrity diagnostics in applications to every element. Such idea for "smart" monitoring systems, including justified requirements for monitoring and prognosis, is a base line of the last standards of system engineering ISO/IEC/IEEE 15288, ISO 13379, ISO 13381, ISO 17359, IEC 61508, etc. Now there is no rather universal analytical approach, widely applicable in different areas for processing data in "smart" monitoring systems, to implement this idea yet. Considering an actuality of the outlined problematics, the universal approach, based on the original models and allowing to define and rationale preventive measures of supporting reliability and safety, is proposed. The approach develops the existing approaches [2, 4, 9-18].

2. The description of the approach

The approach includes the next 5 Steps.

Step 1 is to define universal formal technologies for logic describing the processes of occurring and activating dangers, diagnostics and recovering system integrity. Technologies should consider the possibilities of periodic control and monitoring and allow to create the probabilistic models of these processes. Performing step 1 two general technologies are proposed: technology 1 (periodical diagnostics of system integrity without the continuous monitoring between diagnostics) and technology 2 (continuous monitoring between periodical diagnostics is added to technology 1). It is technology 1 in special case of technology 2– see Figure 1.

Note. 1. System integrity is defined as such system state when system purposes are achieved with the required quality (including reliability) and/or safety. 2. It is supposed that used diagnostic tools allow to provide system integrity recovery after revealing the dangers or the consequences of influences.

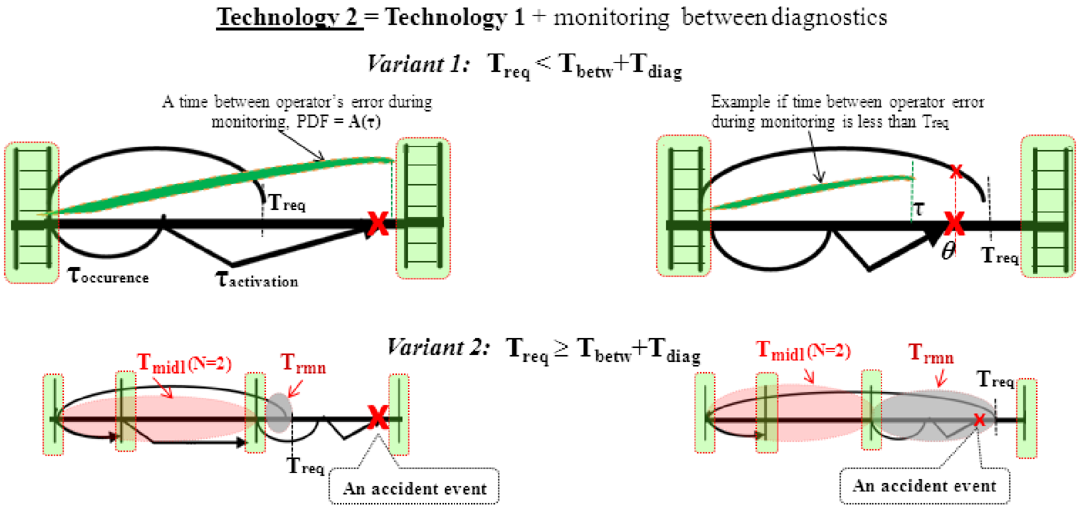

Technology 2 = Technology 1 + monitoring between diagnostics
Variant 1: $T_{req} < T_{betw} + T_{diag}$
A time between operator's error during monitoring, PDF = A(τ)
T_{req}
$\tau_{occurence}$
$\tau_{activation}$
Example if time between operator error during monitoring is less than Treq
τ
θ
T_{req}
Variant 2: $T_{req} \geq T_{betw} + T_{diag}$
T_{midl} (N=2)
T_{rmn}
T_{req}
An accident event
T_{midl} (N=2)
T_{rmn}
T_{req}
An accident event

Figure 1. Some accident events for technology 2 (left – "correct operation", right – "a loss of integrity" during given time for prediction $T_{req.}$)

Technology 1 is based on the periodical diagnostics of a system integrity. Diagnostics are carried out to detect the dangers occurrences into a system or the consequences of their negative influences. The lost system integrity can be detected only as a result of diagnostic, after which a recovery of integrity is started. Dangerous influence on a system operating correctly is performed step-by step: an activation time of danger begins after this danger occurrence in a system (correct operation is continued yet), a danger influence (an accident event) begins after finishing activation time – it means a loss of integrity. A system integrity can't be lost before an occurred danger is activated, activation means this danger has influenced on a system. Otherwise the danger will be detected and neutralized during the next diagnostic time and recovering works.

Technology 2, unlike the previous Technology 1, implies that operators (a man or software system or robot or special device or their combination) trace system integrity between diagnostics. In case of detecting a danger an operator initiate a recovery of system integrity (dangers removing and system recovery are the same as for Technology 1). Faultless operator's actions provide a neutralization of a danger. Diagnostic measures are periodically performed and also operator possibilities are enough for recovering. A danger influence is possible only if operator makes an error (it means the possibilities for detecting are finished) and dangerous influence occurs before the next diagnostic time.

Step 2 is to define universal elementary ranges for the traced parameters (from reliability or safety point of view), monitored conditions and interpretation of events, allowing analytical data processing by probabilistic modeling.

Step 3 is to develop probabilistic models for Technologies 1, 2, which can be used for "Black Box", and the methods to generate new probabilistic models for complex structures, allowing prognostic researches on a level of the probability destribution function (PDF) of time before a next abnormality for one element, subsystem, system.

Step 4 is to implement the proposed probabilistic models and methods of step 3 for processing data in "smart" monitoring system, to define acceptable risks.

Step 5 is to estimate effects from a use of preventive measures in real time (by probabilistic models implemented on step 4) and to define rational preventive measures of supporting reliability and safety by solving optimization problems with limits on acceptable risks.

The implementation of Steps 1 – 5 is described below.

3. The proposed probabilistic models and methods (Step 3)

3.1 The Models for "Black Box"

The probability of system operation with required reliability and/or safety within the given prognostic period (i.e. probability of success) may be estimated as a result of use the models for technologies 1 and 2 (described above). Assumption: for all time input characteristic the probability distribution functions exist. Considering consequences risk $R(T_{req})$ to lose integrity (safety, quality or separate property, for example – reliability) is addition to 1 for probability $P(T_{req})$ of probability of success – see Figures 1 and 2. $R(T_{req}) = 1 - P(T_{req})$, consequences are considered accordingly.

There are possible the next variants for technologies 1 and 2: variant 1 – the given prognostic period T_{req} is less than established period between neighboring diagnostics ($T_{req} < T_{betw}+T_{diag}$); variant 2 – the given prognostic period T_{req} is more than or equals to established period between neighboring diagnostics ($T_{req} \geq T_{betw}+T_{diag}$). Here T_{betw} – is time between the end of diagnostic and the beginning of next diagnostic, T_{diag} – is the diagnostic time including recovering if it needs. The next formulas for PDF of time between the losses of system integrity are proposed for using [2, 4, 14-18].

PDF for the model of technology 1, variant 1: Under the condition of independence for input characteristics the probability of providing system integrity (i.e. probability of success) for variant 1 is equal to

$$P_{(1)}(T_{req}) = 1 - \Omega_{occur} * \Omega_{activ}(T_{req}), \qquad (1)$$

where $\Omega_{occur}(t)$ – is the PDF of time between neighboring occurrences of danger; $\Omega_{activ}(t)$ – is the PDF of activation time of occurred danger. These PDF $\Omega_{occur}(t)$ and $\Omega_{activ}(t)$ may be exponential PDF - see rationale in [2, 4, 14-15]. For different threats a frequency of dangers for these PDF is the sum of frequencies of every kind of threats.

PDF for the model of technology 1, variant 2. Under the condition of independence for input characteristics the probability of providing system integrity (i.e. probability of success) for variant 2 is equal to

$$P_{(2)}\,(T_{req}) = N((T_{betw}+T_{diag})/T_{req})\; P_{(1)}{}^{N}(T_{betw}+T_{diag}) + (T_{rmn}/T_{req})\; P_{(1)}(T_{rmn}), \quad (2)$$

where $N=[T_{req.}/(T_{betw}+ T_{diag.})]$ – may be real (for PDF) or the integer part (for estimation of deviations), $T_{rmn} = T_{req} - N(T_{betw}+T_{diag})$.
The probability of providing system integrity within the given time $P_{(1)}(T_{req})$ is defined by (1).

PDF for the model of technology 2, variant 1. Under the condition of independence for input characteristics the probability of providing system integrity for variant 1 is equal to

$$P_{(1)}(T_{reg}) = 1 - \int_{0}^{T_{req.}} dA(\tau) \int_{\tau}^{T_{req.}} d\,\Omega_{penetr} * .\Omega_{act..}(\theta) \quad . \qquad (3)$$

Here A(τ) is the PDF of time between operator’s error. A(τ) may be exponential PDF [2, 4, 14-15].

PDF for the model of technology 2, variant 2. Under the condition of independence of characteristics the probability of providing system integrity for variant 2 is equal to

$$P_{(2)}\,(T_{req}) = N[(T_{betw}+T_{diag})/T_{req}]\; P_{(1)}{}^{N}(T_{betw}+T_{diag}) + (T_{rmn}/T_{req})\; P_{(1)}(T_{rmn}), \quad (4)$$

where the probability of providing system integrity within the given time $P_{(1)}(T_{req.})$ is defined by (3).

The final clear analytical formulas for calculating are received by Lebesque-integration of (3) expression. The models are applicable to the system presented as one element. The main result of such system modeling is the probability of providing system integrity during the given period of time.

The method of forming PDF is the next: if probabilities for all points $T_{req.}$ from 0 to ∞ will be calculated, a trajectory of the PDF P(t) is automatically synthesized for t from 0 to ∞.

3.2 Integration of probabilistic models for complex structures

The main output of modelling by models 3.1 is a trajectory of the PDF depending on characteristics of threats, periodic diagnostics, monitoring and recoveries. And the building of such PDF is the real base to predict probability P and risk R for the time points $T_{req.}$. It is important to know a mean time between neighbouring losses of integrity like mean time between neighbouring failures in reliability (MTBF), but in application to safety, quality etc.

For complex systems with parallel or serial structure existing models with known PDF can be developed by usual methods of probability theory [19-20 etc.]. Let's consider the elementary structure from two independent parallel or series elements. Let’s PDF of time τ_i between losses of i-th element integrity is $B_i(t)$, i.e. $B_i(t) = P(\tau_i \leq t)$, then:

1) time between losses of integrity for system combined from series connected independent elements is equal to a minimum from two times τ_i: failure of 1st or 2nd elements (i.e. the system goes into a state of lost integrity when either 1st, or 2nd element integrity is lost). For this case the PDF of time between losses of system integrity is defined by expression

$$B(t) = P(\min(\tau_1,\tau_2) \leq t) = 1 - P(\min(\tau_1,\tau_2) > t) = 1 - P(\tau_1 > t)P(\tau_2 > t) = \\ = 1 - [1-B_1(t)]\,[1-B_2(t)]; \qquad (5)$$

2) time between losses of integrity for system combined from parallel connected independent elements (with hot reservation) is equal to a maximum from two times τ_i: failure of 1st and 2nd elements (i.e. the system goes into a state of lost integrity when both 1st and 2nd elements have lost integrity). For this case the PDF of time between losses of system integrity is defined by expression

$$B(t) = P(\max(\tau_1,\tau_2) \leq t) = P(\tau_1 \leq t)P(\tau_2 \leq t) = B_1(t)B_2(t). \qquad (6)$$

Applying recurrently expressions (5)–(6) it is possible to build PDF of time between losses of integrity for any complex system with the combination of parallel and/or series structures.

All these ideas for analytical modelling operation processes are supported by the software tools “Mathematical modelling of system life cycle processes” – “know how” (registered by Rospatent №2004610858), “Complex for evaluating quality of production processes” (registered by Rospatent №2010614145) and others [2, 4, 14, 15].

3.3 About methods for optimization

By using the models and software tools above the problems of optimization for an element, subsystem, system can be solved through the calculations of the probability of providing system integrity or the risk to lose system integrity during given prognostic period on time line. This approach considers the different threats, conditions and the measures of counteractions in applications to every element, subsystem and to whole “smart” system. The given acceptable risk can be established

by precedent principle. Thus the final choice of integrated measures is allocated on a payoff to a customer in a view of a specificity of created or maintained system.
For example, the next general formal statements of problems for optimization can be used:

1) for the stages of “smart” system creation: system parameters, technical and management measures, represented in the terms of the time characteristics of threats, control and/or conditions monitored and a comprehensible recovery of lost integrity are the most rational for the given prognostic period if the minimum of expenses for creation of system is reached at limitations on acceptable levels of risks to lose integrity (for elements, subsystems, whole system) and considering other development, operation or maintenance conditions and limitations;

2) on operation and maintenance stages: system parameters, technical and management measures, represented in the terms of the time characteristics of threats, control and/or conditions monitored and a comprehensible recovery of lost integrity are the most rational for the given prognostic period if the maximum operation profit is reached at limitations on acceptable levels of risks and considering other operation or maintenance conditions and limitations.

The combination of these formal statements also can be used in system life cycle. The proposed models and methods are applicable to be used in real time and also for short- and long-term planning. It is demonstrated by examples.

4. Examples of implementation for processing data in “smart” monitoring system (with the demonstrations of Steps 1-5)

Example 1 for demonstration of Steps 1-5 implementation [15-18]. In 2016 the “smart” remote monitoring system (RMS) was designed for the Joint-Stock Company “Siberian Coal Energy Company” (“SUEK” – www.suek.ru). Because of thousands of system elements and subsystems should be covered by monitoring, universal formal technologies for logic describing the processes of occurring and activating dangers, diagnostics and recovering the integrity of the values of parameters, maintained conditions for coal miners, normal operation of machinery, equipment and whole mine are established. The Technologies 1 and 2 above are met formal logic processes. It means the implementation of Step 1.

The implemented Step 2 is explained by the next propositions. Monitored parameters have been chosen for all valuable conditions, machinery and equipment. For each parameter the ranges of possible values of conditions are established: “Working range inside of norm”, “Out of working range, but inside of norm”, “Abnormality”, it may be interpreted by similarly light signals – "green", "yellow", "red" – see Figure 2. The condition “Abnormality” characterizes a threat to lose system integrity after danger influence (on logic level this range “Abnormality” may be interpreted as failure, fault, unacceptable risk or quality, etc.). This construction allows to extract data for probabilistic modeling: time between moments of the occurrences of dangers (potential threats), activation time of occurred dangers, recovery time.

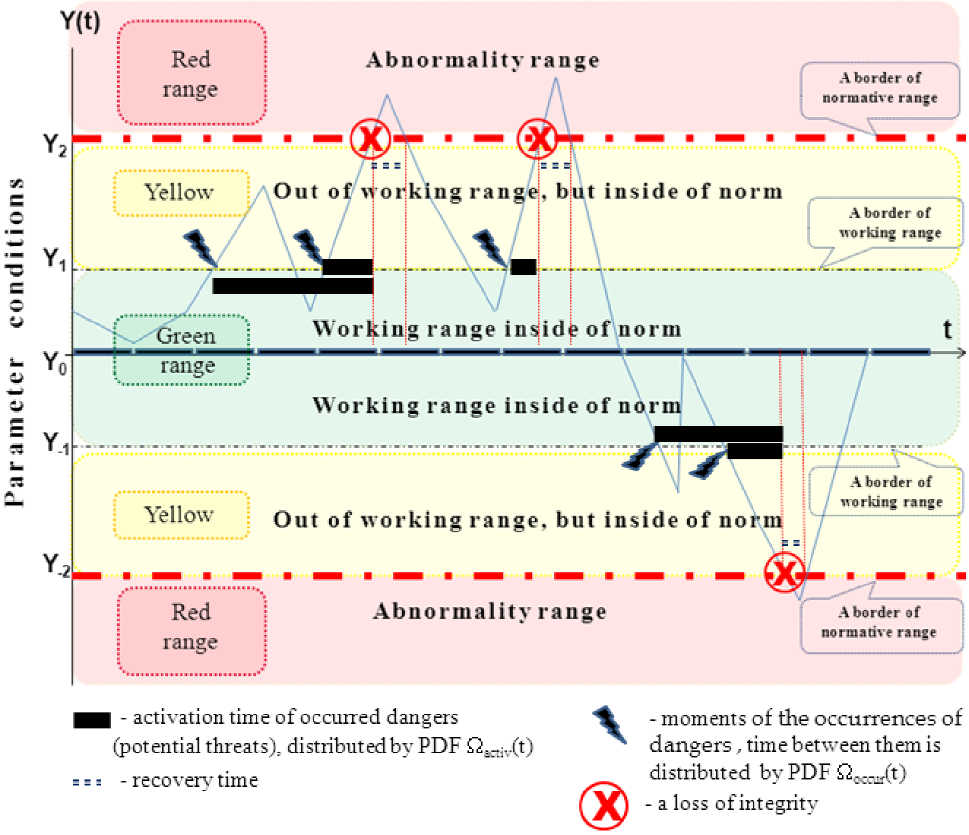

Y(t)
Parameter conditions
Red range
Abnormality range
A border of normative range
Y2
Yellow
Out of working range, but inside of norm
A border of working range
Y1
Green range
Working range inside of norm
t
Y0
Working range inside of norm
Y-1
A border of working range
Yellow
Out of working range, but inside of norm
Y-2
Red range
Abnormality range
A border of normative range
- activation time of occurred dangers (potential threats), distributed by PDF Ωactiv(t)
- recovery time
- moments of the occurrences of dangers, time between them is distributed by PDF Ωoccur(t)
- a loss of integrity

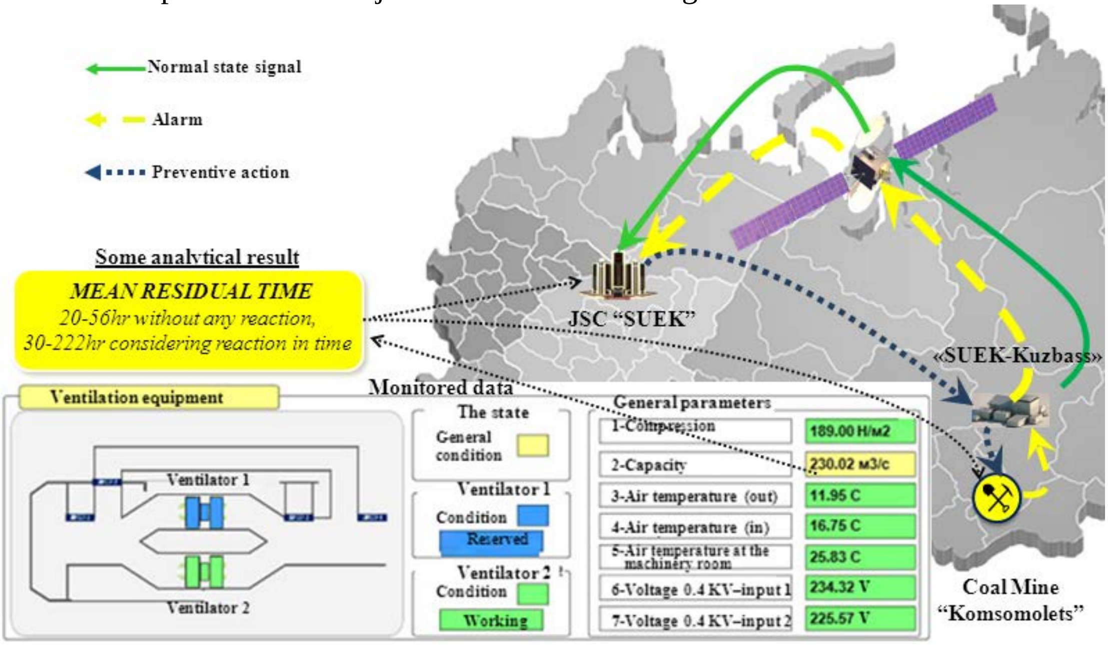
Figure 2. The universal elementary ranges for traced parameters

All parameters are represented as the system elements. The conditions for coal miners, operating machinery and equipment are represented as complex subsystems integrated from serial elements (serial structure) and parallel subsystems for reservation (parallel structure). The whole mine is represented as complex system integrated from serial and parallel structures. Logic interpretation for serial structure from two elements is: the structure goes into a state of lost integrity when either 1st or 2nd element integrity is lost. Logic interpretation for parallel structure from two subsystems is: the structure goes into a state of lost integrity when both 1st and 2nd subsystems integrities are lost.

Step 3 has allowed to do the adaptation of proposed probabilistic models and methods (models “Black Box” for Technologies 1, 2 and the methods to generate new probabilistic models for complex structures, allowing prognostic researches on a level of PDF of time before a next abnormality) for implementing to parameters, valuable conditions, machinery and the equipment of the whole mine. Considering consequences risk R(T_{req}) to lose integrity means probability to be though one time in “red” range during period T_{req} – see Figures 1 and 2. PDF $\Omega_{occur}(t)$ of time between neighboring occurrences of danger (from the “green” at the “yellow” range), PDF $\Omega_{activ}(t)$ of activation time of occurred danger (the time from the 1-st occurrence at the “yellow” range to the 1-st occurrence at the “red” range) and PDF A(τ) of time between operator’s error are approximated by exponential PDF – input for mean time see from Figure 2 and from the processing of statistics.

Step 4 has allowed to implement proposed probabilistic models and methods by the software of “smart” RMS, to define acceptable risks. RMS is intended for a possibility of prediction and the prevention of possible emergencies, minimization of a role of human factor regarding control and supervising functions. It may be reached on the basis of gathering and analytical processing in real time the information on controllable parameters of conditions, machinery and monitored equipment.

Step 5 has allowed to to estimate effects from a use of preventive measures in real time and to define rational preventive measures of supporting reliability and safety by solving optimization problems with limits on acceptable risks. Effects are reached on the basis of gathering and analytical processing in real time the information on controllable parameters of objects monitored – see Figure 3.



1-Compression	189.00 H/м2
2-Capacity	230.02 м3/c
3-Air temperature (out)	11.95 C
4-Air temperature (in)	16.75 C
5-Air temperature at the machinery room	25.83 C
6-Voltage 0.4 KV–input 1	234.32 V
7-Voltage 0.4 KV–input 2	225.57 V

Figure 3. Example of implementation

The proposed probabilistic models and methods help to predict in real time the mean residual time before the next parameters abnormalities for two different cases: without any reaction of responsible staff and if obligatory adequate reaction is always.

Example 2 for “Black Box”. Let the mean time between neighboring occurrences of danger (from the “green” at the “yellow” range) is 1 month, i.e. T_{occur} =1month, T_{diag} =$T_{err.}$=0. The case “without any reaction” after parameter transition from “green” into “yellow” range is characterized by input T_{betw} =1year, and the input T_{betw}=8hours (about every shift) characterizes the case “for obligatory adequate reaction in real time”. The result of the prediction of the mean residual time before the next parameters abnormalities (see Figure 3) helps to define rational preventive measures of supporting safety in real time [16, 17].

Analytical results of RMS operation for responsible staff is transparent for all interested parties and adequate preventive reaction in time allows to increase a mean residual time before the next parameters abnormalities.

Example 3 (for complex structure). Let's analyse a fragment of the main gas pipeline Bovanenkovo-Ukhta (more than 1200 km) by probabilistic modelling of natural and technogenic processes. It constructed over an earth surface. Sub-fragments between compressor stations (9 stations - Bajdaratsky, Jarynsky, Gagaratsky, Vorkuta, Usinsk, Intinsky, Syninsky, Chikshinsky, Maloperansky) are allocated. There are serial subsystems and every subsystem has parallel structure of elements (pipeline) - see Figure 4, 5.

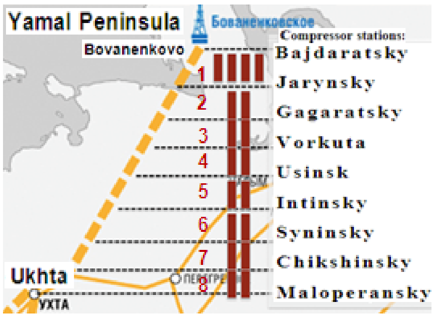


Figure 4. The analyzed fragment of the main gas pipeline

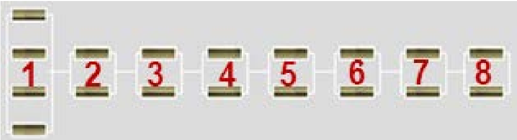


Figure 5. The serial-parallel structure for modelling processes

About 75-90% from the pipelines are under natural threats, including ice drift (threats for constructions). It is required to estimate risk to lose integrity (quality of operation) of fragment Bovanenkovo-Ukhta in 2023-2043.

The solving of a problem is the next [15-16]. According to estimations of experts, in 20-30 years there will be considerable changes of climatic conditions which will cause rise in temperature of frozen thicknesses, increase in depth seasonal thawing and, as consequence, decrease in stability and bearing ability of the bases for a gas pipeline and other engineering constructions. Technical characteristics of elements between compressor stations are considered as identical, except for the first subfragment (between stations Bajdaratsky and Jarynsky) which is underwater transition (reservation by 4 elements-pipelines) – see Figure 4. Initial data for modelling have been generated depending on conditions of concrete sites and specificity of a territorial arrangement of a line.

Results of modelling processes have shown, that risk to lose integrity (quality of operation) for 20 prognostic years during the period 2023-2043 is equal to 0.6 – 0.8. In comparison with other precedents these figures speak about expediency of undertaking of preventive measures, and also about the necessity of working out the Plan of emergencies liquidation. If period between system controls will be reduced from 6 to 3 months the risk to lose integrity in 2023-2043 is nearby 0.16 – 0.44. It is twice more low, rather than for an existing mode of maintenance and repair. On the basis of these results the following recommendations are scientifically proved:
- to establish a risk level to lose integrity (quality of operation) 0,38 within 10 years of operation as unacceptable (on the base of «precedent principle»);
- to pass to the quarterly control of a condition of system after 10 years of operation (i.e. since 2024);

- to use annual planning of maintenance measures service on the basis of modeling processes for rational risk management in acceptable limits.

Example 4. What about the possible pragmatic effects? (Step 5)

The Complex (as a part of global system) of risks predictions for techno-genic safety support on the objects of oil & gas distribution has been awarded by Award of the Government of the Russian Federation in the field of a science and technics for 2014. The created peripheral posts are equipped additionally by the means of Complex to feel vibration, a fire, the flooding, unauthorized access, hurricane, and also the intellectual means of adequate reaction, capable to recognize, identify and predict a development of extreme situations. The applications of Complex for 200 objects in several regions of Russia during the period 2009-2014 have already provided economy about 8,5 Billions of Roubles. The economy is reached at the expense of effective implementation of the functions of risks prediction and processes optimization [2, 4, 14-16].

Conclusion

The universal approach, applicable in different areas for processing data in “smart” monitoring systems and based on the original probabilistic models, is proposed. The approach includes the next 5 Steps:
- Step 1 - to define universal formal technologies for logic describing the processes of occurring and activating dangers, diagnostics and recovering system integrity, considering the possibilities of periodic control and monitoring;
- Step 2 - to define universal elementary ranges for the traced parameters (from reliability or safety point of view), monitored conditions and interpretation of events, allowing analytical data processing by probabilistic modeling;
- Step 3 - to develop probabilistic models for two Technologies, which can be used for “Black Box”, and the methods to generate new probabilistic models for complex structures, allowing prognostic researches on a level of the probability destribution function (PDF) of time before a next abnormality for one element, subsystem, system;
- Step 4 - to implement the proposed probabilistic models and methods of step 3 for processing data in “smart” monitoring system, to define acceptable risks;
- Step 5 - to estimate effects from a use of preventive measures in real time and to define rational preventive measures of supporting reliability and safety by solving optimization problems with limits on acceptable risks.

Implementation of the approach for processing data in “smart” monitoring system allows to define rational preventive measures of supporting reliability and safety. They proposed models and methods are applicable to be used in real time and also for short- and long-term planning.

The efficiency of approach is demonstrated by the examples of implementation in the for the Joint-Stock Company “Siberian Coal Energy Company”, for a fragment of the main gas pipeline Bovanenkovo-Ukhta, for the Complex of risks predictions for techno-genic safety support on the objects of oil & gas distribution (applications of which for 200 objects in several regions of Russia during the period 2009-2014 have provided the economy about 8,5 Billions of Roubles).

References

[1] Kostogryzov, A., Nistratov A., Zubarev, I., Stepanov, P., Grigoriev, L. (2015) About accuracy of risks prediction and importance of increasing adequacy of used probabilistic models. *Journal of Polish Safety and Reliability Association. Summer Safety and Reliability Seminars,* Volume 6, Numbers 2, 2015, pp. 71-80.

[2] Kostogryzov A., Nistratov G. (2004) *Standardization, mathematical modelling, rational management and certification in the field of system and software engineering" (80 standards, 100 mathematical models, 35 software tools, more than 50 practical examples).* Armament. Policy. Conversion, Moscow.

[3] Zio E. (2006) An Introduction to the Basics of *Reliability and Risk Analysis.* World Scientific.

[4] Kostogryzov, A. and Stepanov, P. (2008) *Innovative management of quality and risks in systems life cycle.* Armament. Policy. Conversion, Moscow.

[5] Kolowrocki, K., Soszynska-Budny, J. (2011) *Reliability and Safety of Complex Technical Systems and Processes.* Springer-Verlag London Limited.

[6] Eid, M. and Rosato, V. (2016) *Critical Infrastructure Disruption Scenarios Analyses via Simulation*. Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, SpringerOpen, pp. 43-62.

[7] Di Pietro, A., Liberto, C., Flourentzou, N., Kyriakides, E., Pothof , I. and Valenti, G. (2016) *Physical Simulators of Critical Infrastructures*. Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, SpringerOpen, pp. 63-84.

[8] Huiskamp, W. and van den Berg, T. (2016) *Federated Simulations.* Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, SpringerOpen, pp. 109-138.

[9] Kostogryzov, A., Nistratov, G., Kleshchev, N. (2006) Mathematical Models and Software Tools to Support an Assessment of Standard System Processes. *Proceedings of the 6th International SPICE Conference on Process Assessment and Improvement,* Luxembourg, pp. 63-68

[10] Kostogryzov, A., Nistratov, G. (2006) Mathematical Models and Software Tools for Analyzing System Quality and Risks according to standard requirements. *Proceedings of the 6th International scientific school "Modelling and Analysis of safety and risk in complex systems" (MASR – 2006),* Saint Petersburg, Russia, July 4 - 8, pp. 155-163.

[11] Grigoriev, L.I., Kershenbaum, V. and Kostogryzov, A. (2010) *System foundations of the management of competitiveness in oil and gas complex.* National Institute of oil and gas, Moscow.

[12] Kostogryzov A., Krylov V., Nistratov A., Nistratov G., Popov V., Stepanov P. (2011) Mathematical models and applicable technologies to forecast, analyze and optimize quality and risks for complex systems, *Proceedings of the 1st International Conference on Transportation Information and Safety (ICTIS), June 30-July 2,2011,* Wuhan, China, pp. 845-854.

[13] Kostogryzov, A., Nistratov, A., Nistratov, G. (2012) Applicable Technologies to Forecast, Analyze and Optimize Reliability and Risks for Complex Systems // *Proceedings of the 6th International Summer Safety and Reliability Seminar*, September 2012, Poland, V.3, No.1, pp. 1-14.

[14] Kostogryzov, A., Nistratov, G. and Nistratov, A. (2012) *Some Applicable Methods to Analyze and Optimize System Processes in Quality Management*. Total Quality Management and Six Sigma, InTech, pp. 127-196.

[15] Abrosimov, N., Kostogryzov, A., Mahutov, N. at al. (2015) Security of Russia. *Legal, Social&Economic and Scientific&Engineering Aspects. The Scientific Foundations of Technogenic Safety*. Under the editorship of N. Mahutov N.A. – Znanie, Moscow.

[16] Artemyev, V., Kostogryzov, A., Rudenko, Ju., Kurpatov, O., Nistratov, G., Nistratov, A. (2017) Probabilistic methods of estimating the mean residual time before the next parameters abnormalities for monitored critical systems. *Proceedings of the 2nd International Conference on System Reliability and Safety (ICSRS)*, Milan, Italy, December 20-22, 2017,pp. 368-373

[17] Artemyev, V., Rudenko, Ju., Nistratov, G. (2018) *Probabilistic methods and technologies of risks prediction and rationale of preventive measures by using "smart systems". Applications to coal branch for increasing Industrial safety of enterprises.* Probabilistic modeling in system engineering. InTechOpen, 2018, pp.23-51.

[18] Kershenbaum, V., Grigoriev, L., Kanygin, P., Nistratov, A. (2018) *Probabilistic modeling processes for oil and gas systems*. Probabilistic modeling in system engineering. InTechOpen, 2018, pp. 55-79.

[19] Feller, W. (1971) *An Introduction to Probability Theory and Its Applications*, Vol. II, Willy.

[20] Klimov, G. (1983) *Probability theory and mathematical statistics,* Moscow State University, Moscow.

A Markov chain model for floods and earthquakes

Mario Lefebvre
Polytechnique Montréal
2500, chemin de Polytechnique
H3T 1J4, Montréal, Canada

Abstract

A Markov chain having three possible states is proposed for the worldwide variations of floods from month to month. After having estimated the transition probabilities of the chain using real-life data, we compute its limiting probabilities. The data set is then divided into two parts and the same calculations are made in order to detect any sign of climate change. Next, the same type of analysis is performed in the case of major earthquakes. The aim is to determine the long-term behaviour of the yearly occurrences of major earthquakes. In the case of floods, the monthly variations seem to occur almost at random. However earthquakes, and especially major ones, show a clear upward trend, which is a major threat for vital services providers. This work could be extended to other important threats.

Keywords: modelling, forecasting, limiting probabilities, climate change.

1. Introduction

Important threats to the continuity of vital services are major floods and earthquakes. Various authors have proposed stochastic processes as models for hydrological and geological events. In hydrology, the author used diffusion and filtered Poisson or renewal processes as models for river flows. The aim was to forecast the flow values a few days in advance (see Lefebvre, 2002a, and Lefebvre and Guilbault, 2008, in particular) or the values of the successive peak flows (Lefebvre, 2002b).

In the case of major earthquakes, many authors have tried to forecast their occurrences and magnitudes; see, for example, Sadeghian (2012), Mostafaei and Kordnoori (2013), Panorias et al. (2016), Votsi et al. (2010) and Votsi et al. (2014).

In this paper, we will use a discrete-time Markov chain having three possible states to model the worldwide variations of major floods from month to month. Similarly, the same model will be used for the worldwide variations of earthquakes from month to month, and finally for major earthquakes from year to year. Once the transition probabilities of the Markov chains have been estimated by making use of real-life data, we will calculate the limiting probabilities of these chains. This will enable us to forecast the behaviour of the variables of interest. Moreover, the data sets will be divided into two parts and the analysis will be performed on each part to detect signs of climate change.

In the next section, the required mathematical background will be presented. Then, the model will be implemented for floods and earthquakes in Sections 3 and 4, respectively. We will conclude this paper with a few remarks in Section 5.

2. Mathematical background

A *stochastic (*or *random) process* is a set of random variables: $\{X(t): t \in T\}$. In general,
t is interpreted as time, and T is a subset of the real numbers. We often choose the subsets $T = \{0, 1, 2, \ldots\}$ or $[0, \infty)$. We say that $X(t)$ is the value or the *state* of the stochastic process at time t.

In the case when $T = \{0, 1, 2, \ldots\}$, the stochastic process is said to be a discrete-time process, and we usually write X_n for the value of the process at time n.

In this paper, we will assume that the *state space* of the stochastic process $\{X_n, n = 0, 1, 2, \ldots\}$ is the set $S = \{0, 1, 2\}$. That is, we assume that for any n, $X_n = 0$, 1 or 2. These values will actually be a coding system.

Next, a discrete-time *Markov chain* is a stochastic process such that

$$P[X_{n+1} = j | X_n = i, X_{n-1} = i_{n-1}, \ldots, X_0 = i_0] = P[X_{n+1} = j | X_n = i], \tag{1}$$

for all states $i_0, \ldots, i_{n-1}, i, j$ in S and for any n. We say that the *future* (n+1), given the *present* (n) and the *past* (n-1, …, 0), depends only on the present.

Moreover, it is usually assumed that the *conditional probability* $P[X_{n+1} = j | X_n = i]$ does not depend on n, so that the process is *time-homogeneous*. We then define the *transition probabilities*

$$p_{i,j} = P[X_{n+1} = j | X_n = i]. \tag{2}$$

The matrix

$$\boldsymbol{P} = (p_{i,j}), i, j \in S \tag{3}$$

is called the *transition matrix* of the Markov chain.

Remark. The above definition can be generalized by assuming, for example, that the value of X_{n+1} depends on both X_n and X_{n-1}. Then, we can define $Z_n = (X_n, X_{n-1})$. Therefore, in the case when $X_n = 0$, 1 or 2 for any n, there would be 9 possible states, that we can denote by 0, 1, …, 8.

Notice that *i* can be equal to *j* in the definition of $p_{i,j}$. That is, the process can make a transition from a given state to the same state. Let K_i denote the number of time units that the process spends in state i before it moves to a different state. We have, by independence:

$$P[K_i = k] = (p_{i,i})^{k-1}\left(1 - p_{i,i}\right) \tag{4}$$

for k = 1, 2, 3, … We say that the random variable K_i has a *geometric distribution* with parameter $p := 1 - p_{i,i}$.

If the model that we propose is realistic, the *histograms* of the variables K_i, for i = 0, 1, 2, should look like the one in Figure 1, in which a decreasing exponential function has been added. A geometric random variable is actually the integer part (+ 1) of an exponential random variable.

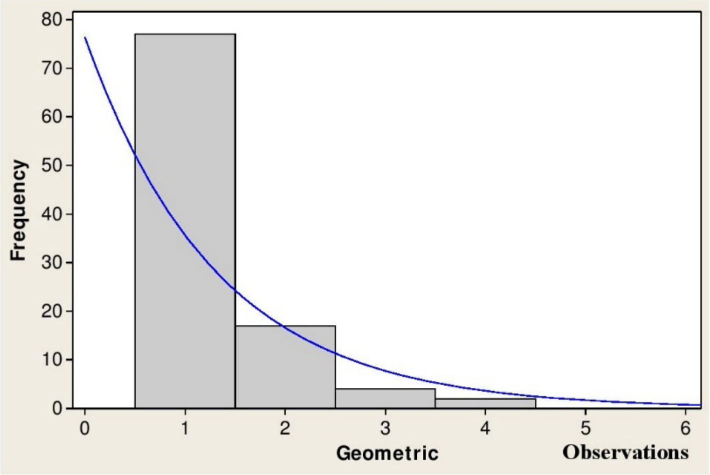


Figure 1. An example of a geometric distribution.

Under some conditions (that will be fulfilled in this paper), we can define the *limiting probability* that the process will be in state *i* when it is in *equilibrium* as follows:

$$\pi_i = \lim_{n\to\infty} P[X_n = i]. \tag{5}$$

Let $\boldsymbol{\pi} := (\pi_0, \pi_1, \pi_2)$. To obtain the limiting probabilities, we can solve the following system of linear equations:

$$\boldsymbol{\pi} = \boldsymbol{\pi P}, \tag{6}$$

together with the condition

$$\sum_{i=0}^{2} \pi_i = 1. \tag{7}$$

In the next section, the above model will be implemented in the case of major floods.

3. Implementation of the model for floods

On the website of the Dartmouth Flood Observatory (floodobservatory.colorado.edu), it is possible to download a file containing a list of large flood events worldwide from 1985. For each flood, the file provides, in particular, the dates when it began and ended, its severity, the number of dead, etc.

The magnitude of a flood is denoted by *M* and is defined as follows:

$$M = \text{Log}\,(\text{Duration x Severity x Affected Area}), \tag{8}$$

in which the Duration is in days, the Affected Area in square kilometers and the Severity is equal to 1, 1,5 or 2 for large, very large and extreme events, respectively.

There are 4536 events in the list. The total number of floods having a value *M* greater than 4 is equal to 3999, and for 1257 floods *M* is greater than 6. A flood with an *M > 4* is considered as *severe*, and one with an *M* > 6 is *very severe*. Hence, the vast majority of the floods that are listed are at least severe.

We used the data for the years 2000 to 2016 (because 2017 is not complete), which is a long enough period. There are 2825 floods in the data set. The average number of floods per month is 13,85.

Let F_n be the number of floods during month *n*. We want to model the variations in the total monthly floods as a discrete-time Markov chain having the following three states:

- 0: if $F_n - F_{n-1} < -2$,
- 1: if $-2 \leq F_n - F_{n-1} \leq 2$,
- 2: if $F_n - F_{n-1} > 2$.

With these states, we obtained the histograms shown in Figures 2-4 for the variables K_0, K_1 and K_2, respectively. We see that the three histograms are quite similar to the one presented in Figure 1. Hence, we may conclude that the model is realistic.

Next, we estimated the various transition probabilities $p_{i,j}$. The estimated transition matrix is

$$\boldsymbol{P} = \begin{pmatrix} 1/6 & 19/66 & 6/11 \\ 9/34 & 27/68 & 23/68 \\ 37/68 & 23/68 & 2/17 \end{pmatrix}. \tag{9}$$

Then, we computed the limiting probabilities:

$$\pi_0 = 0{,}3257, \qquad \pi_1 = 0{,}3420, \qquad \pi_2 = 0{,}3324. \tag{10}$$

Thus, based on the data set that we used, in the long run the number of floods during a given month is almost as likely to increase or to decrease by more than 2, or to be within the interval [-2, 2], compared with the previous month. Moreover, the average value of F_n - F_{n-1} is 0,0345. One must therefore conclude that there has not been a significant change in the number of major floods worldwide during the period 2000-2016, and that the variations from month to month occur rather at random.

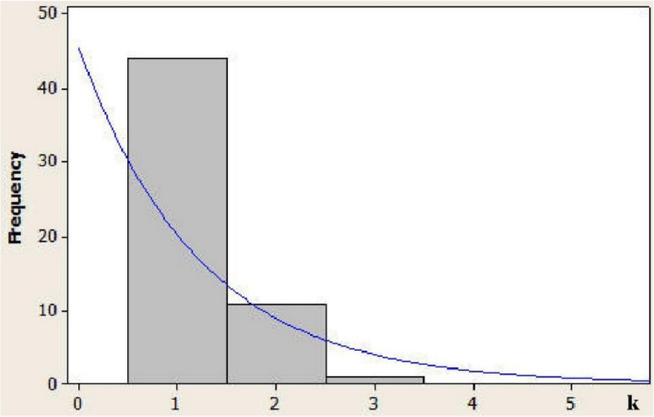


Figure 2. Histogram of the variable K_0 in the case of major floods, with the observed values (k) on the x-axis and the corresponding frequencies on the y-axis.

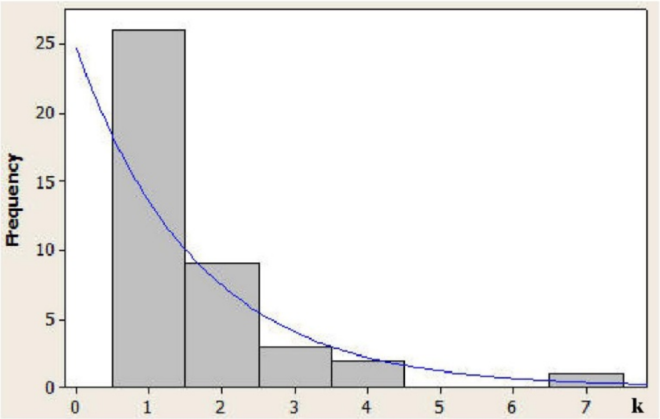


Figure 3. Histogram of the variable K_1 in the case of major floods.

To check whether there have been some significant changes between the beginning and the end of the time period considered, we divided the data set into two parts: from 2000 to 2007, and then from 2008 to 2016, and we calculated the limiting probabilities in each case. The results are presented in Table I. We see that the limiting probabilities are quite similar, especially when we take into account the fact that the results are less reliable when the data set is smaller. Notice that there are actually less variations during the period 2008-2016, since state 1 has the largest limiting probability. This seems to be confirmed by the fact that the standard deviation of the monthly variations decreased
from 7,54 (2000-2007) to 5,90 (2008-2016). We find that the mean also decreased, from 0,116 to -0,037.

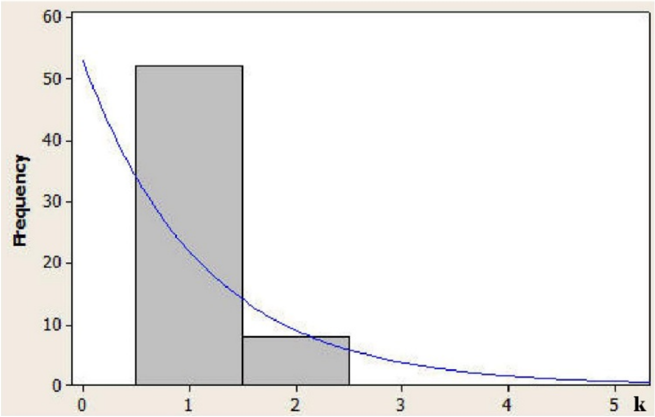


Figure 4. Histogram of the variable K_2 in the case of major floods.

Table I: Limiting probabilities calculated for the periods 2000-2016, 2000-2007 and 2008-2016.

Period	π_0	π_1	π_2
2000-2016	0,3257	0,3420	0,3324
2000-2007	0,3368	0,3263	0,3368
2008-2016	0,3149	0,3575	0,3275

4. Implementation of the model for earthquakes

In the ANSS (Advanced National Seismic System) Composite Catalog, we can find monthly counts of earthquakes of magnitude greater than or equal to 2,5 from various sources (ncedc.org/anss/inventory/anss_catalog.count). We used the data provided by USGS (U.S. Geological Survey) National Earthquake Information Center, for the years 1983 to 2016.

There have been 704.825 earthquakes in the period considered, for an average number of 1725,5 per month, ranging from a minimum of 524 to a maximum of 4173.

Let E_n be the number of earthquakes during month n, and define

$$Y_n = \frac{(E_n - E_{n-1})}{E_{n-1}} \text{ x } 100 \tag{11}$$

for n = 2, 3, … That is, Y_n is the *monthly percentage variation* of earthquakes. We consider a discrete-time Markov chain $\{X_n, n = 2, 3, \ldots\}$ with state space $S = \{0, 1, 2\}$, such that X_n is equal to

- 0: if $Y_n < -10$,
- 1: if $-10 \leq Y_n \leq 10$,
- 2: if $Y_n > 10$.

As in the case of floods, we produced the histograms for the variables K_0, K_1 and K_2. They are presented in Figures 5-7.

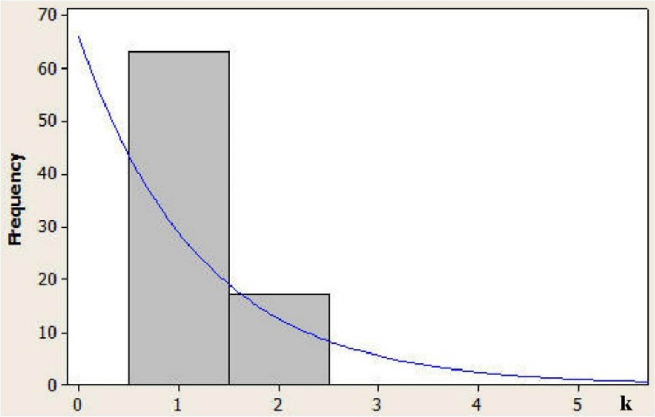


Figure 5. Histogram of the variable K_0 in the case of earthquakes.

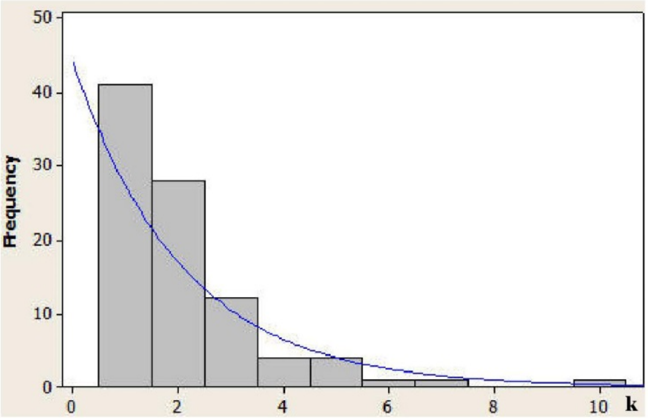


Figure 6. Histogram of the variable K_1 in the case of earthquakes.

We observe that each histogram has approximately the form expected for a random variable having a geometric distribution. We could perform a goodness-of-fit statistical test to reinforce this assertion. However, in the case of K_0 and of K_2 there are not many different values taken by these variables. Therefore, goodness-of-fit tests are less reliable, because the number of *degrees of freedom* is small.

Next, the estimated transition matrix is

$$\boldsymbol{P} = \begin{pmatrix} 17/96 & 13/32 & 5/12 \\ 35/194 & 50/97 & 59/194 \\ 45/116 & 53/116 & 9/58 \end{pmatrix}, \qquad (12)$$

from which we obtain the following limiting probabilities:

$$\pi_0 = 0{,}2394, \qquad \pi_1 = 0{,}4724, \qquad \pi_2 = 0{,}2881. \qquad (13)$$

This time, the π_is are quite different and π_2 is significantly larger than π_0, implying a tendency to have an increase in the number of earthquakes. Furthermore, the average value of the variable Y_n is 1,96%, which is not negligible.

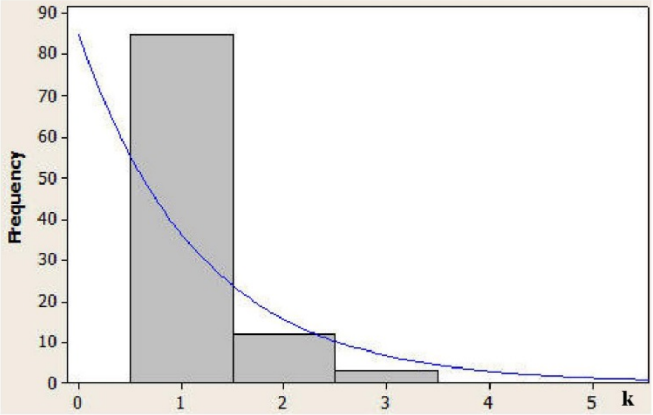


Figure 7. Histogram of the variable K_2 in the case of earthquakes.

In Table II, we present the limiting probabilities obtained by dividing the data set into two parts: 1983-1999 and 2000-2016.

Table II: Limiting probabilities calculated for the periods 1983-2016, 1983-1999 and 2000-2016.

Period	π_0	π_1	π_2
1983-2016	0,2394	0,4724	0,2881
1983-1999	0,2416	0,4820	0,2764
2000-2016	0,2378	0,4619	0,3003

As expected, the limiting probabilities are rather stable, with nevertheless a non-negligible increase in the value of π_2.

4.1 The case of large earthquakes

Large earthquakes are obviously very important threats to the continuity of vital services. We can find a list of earthquakes of magnitude greater than or equal to 6 on the website of USGS (earthquake.usgs.gov/earthquakes). We used the data for earthquakes anywhere in the world between 1980 and 2017, and we modelled the yearly variations again as a discrete-time Markov chain having three possible states.

First, for earthquakes of magnitude of at least 6, in order to obtain the desired histograms for the variables K_i, we defined the states

- 0: if $Y_n < -5$,
- 1: if $-5 \leq Y_n \leq 5$,
- 2: if $Y_n > 5$.

We then estimated the transition probabilities and calculated the limiting probabilities:

$$\pi_0 = 0{,}3056, \qquad \pi_1 = 0{,}4167, \qquad \pi_2 = 0{,}2778. \tag{14}$$

Although the value of π_0 is larger than that of π_2, the average value of Y_n is 1,50%, denoting an upward trend.

Finally, in the case of earthquakes of magnitude equal to 7 or more, the number of observations is much smaller and the yearly variations quite large. Therefore, we defined the states

- 0: if $Y_n < -20$,
- 1: if $-20 \leq Y_n \leq 20$,
- 2: if $Y_n > 20$.

The estimated limiting probabilities are the following:

$$\pi_0 = 0{,}2990, \qquad \pi_1 = 0{,}2186, \qquad \pi_2 = 0{,}4825. \tag{15}$$

Moreover, the average value of Y_n is 5,55%. Thus, the data point to a very significant yearly increase in the percentage variation of very large earthquakes, with almost a 50% chance of having, in the long run, at least 20% more earthquakes of magnitude 7+ than the previous year. The data set covers a 38-year period, and there have been 538 earthquakes of magnitude 7 or more worldwide, for an average of 14,16 per year. Therefore, we can assert that the conclusions that we drew are well supported. Notice that a 20% increase translates into three additional earthquakes of magnitude 7+ per year.

5. Concluding remarks

In this paper, two of the most important threats to the continuity of vital services have been considered, namely major floods and earthquakes. In both cases, it was found that a discrete-time Markov chain with a state space containing three values could be used as a realistic model for the monthly or yearly variations of the events of interest.

Our aim was to use the model proposed in this paper to forecast the long-term behaviour of floods and earthquakes. While in the case of floods, based on reliable real-life data, the monthly variations seem to occur almost at random, earthquakes, and especially major ones, show a clear upward trend, which is obviously worrisome for vital services providers.

As a sequel to this work, one could try to find stochastic models for other important threats, such as hurricanes and tsunamis. On the website Global Risk Data Platform (preview.grid.unep.ch), one can find links to various real-life data sets for a number of natural hazards.

Acknowledgements

This work was supported by the Natural Sciences and Engineering Research Council (NSERC) of Canada.

References

Lefebvre, M. (2002a) Geometric Brownian motion as a model for river flows. *Hydrological Processes*, vol. 16, pp. 1373-1381.

Lefebvre, M. (2002b) Modeling and forecasting the peak flows of a river. *Mathematical Problems in Engineering*, vol. 8, pp. 553-562.

Lefebvre, M. and Guilbault, J.-L. (2008) Using filtered Poisson processes to model a river flow. *Applied Mathematical Modelling*, vol. 32, pp. 2792-2805.

Mostafaei, H. and Kordnoori, S. (2013) The application of the semi-Markov model in predicting the earthquake occurrences in Alborz fault region, Northern Iran. *Earth Science India*, vol. 6, pp. 147-159.

Panorias, C., Papadopoulou, A. and Tsapanos, T. (2016) On the earthquake occurrences in Japan and the surrounding area via semi Markov modeling. *Bulletin of the Geological Society of Greece*, vol. 50, pp. 1535-1542.

Sadeghian, R. (2012) Forecasting time and place of earthquakes using a semi-Markov model: With case study in Tehran province. *Journal of Industrial Engineering International*, vol. 8, pp. 1-7.

Votsi, I., Limnios, N., Tsaklidis, G. and Papadimitriou, E. (2010) Semi-Markov models for seismic hazard assessment in certain areas of Greece. *Bulletin of the Geological Society of Greece*, vol. 43, pp. 2200-2209.

Votsi, I., Limnios, N., Tsaklidis, G. and Papadimitriou, E. (2014) Hidden semi-Markov modeling for the estimation of earthquake occurrence rates. *Communications in Statistics – Theory and Methods*, vol. 43, pp. 1484-1502.

Recoverability Analysis Model for Railway Networks

Ratthaphong Meesit*, John Andrews**, Rasa Remenyte-Prescott***
Resilience Engineering Research Group, University of Nottingham, University Park, Nottingham, UK, NG7 2RD
Email: ratthaphong.meesit@nottingham.ac.uk*, john.andrews@nottingham.ac.uk**, r.remenyte-prescott@nottingham.ac.uk***.

Abstract

The occurrence of unexpected events, such as infrastructure failures and natural disasters, are unavoidable in railway operation. Traffic controllers and train operators are thus required to manage the situation and provide the best possible services for passengers. This paper presents a recoverability analysis model that can be used to evaluate the efficiency of mitigation strategies, short-turning train services and rail replacement bus operation, to enhance the resilience of a railway network during an unplanned-track blockage situation. The model is built using a discrete event simulation technique. Two performance indicators predicted are passenger delay and the cost of bus replacement operation. The computational experiment of the proposed model on the real-world case study shows that these indicators are useful to support a decision-making process during an unplanned disruption.

Keywords: Railway disruption, Short-turning operation, Rail replacement bus operation, Recoverability, Resilience.

1. Introduction

Unplanned events, such as network component failures (e.g. signals and points) or environmental disasters (e.g. floods, strong winds and landslides), are a major issue in the railway network operation. This is because once these events occur, it is difficult to manage resources such as crews and trains to counter the situations. Thus, such events commonly cause delays and cancellations of train services on the network. Even though the railway timetables are generally designed to include buffer times to absorb the impact of these unplanned events, these can only cope with small disruptions, not with severe disruptions that require to close a part of railway track for several hours (Cadarso et al*.*, 2013).

To this end, traffic controllers and train operators need to deal with the real-time situation to ensure the best possible services for passengers (Jespersen-groth et al., 2009). The most widely used strategies during a track blockage situation are short-turning train services on a disrupted route and providing rail replacement bus services to serve stranded passengers at impacted stations. These strategies are commonly organised and implemented based on the experience of traffic controllers and train operators (Ghaemi et al., 2018; Gu et al., 2018). The ad-hoc solution from these strategies may help manage a disruption in a timely manner. However, it might not be the effective solution that can maintain both passenger delays and operating costs to an acceptable level. Therefore, there is a need for developing a model that can support both traffic controllers and train operators to establish a suitable solution during a severe unplanned disruption.

In the past, a great deal of research has been published on the development of recoverability models for railway networks. However, according to Cacchiani et al. (2014), most of the previous studies have focused on handling low impact disruptions (i.e. the application of dispatching rules such as overtaking and changing in stop pattern). Little attention has been paid to supporting the management of a railway network during a blockage situation (Ghaemi et al., 2017). Moreover, in practice the short-turning operation of the trains on the disrupted routes are normally deployed together with the rail replacement bus services. However, previous studies seem to model these strategies separately. For example, the works by Louwerse and Huisman (2014), Veelenturf et al. (2015) and Ghaemi et al. (2018) only focused on the short-turning operations, while the models by Kepaptsoglou and Karlaftis (2009), Jin et al. (2015) and Gu et al. (2018) assumed the operation of a railway network and attempted to design bus replacement services during a disruption. Therefore, a model that can be used to evaluate these mitigation strategies simultaneously is still lacking. The interaction between train and bus operations and the simulation of passengers on the network once both strategies are applied require further studies.

This study presents a new recoverability analysis model that can be applied to simulate the short-turning and rail replacement bus operation during a track blockage situation. The model is developed based on the railway network simulation model by Meesit and Andrews (2018). The discrete event simulation technique is used. The interaction between trains and buses is considered, and the passenger flow within the network is taken into account. Moreover, the key performance indicators predicted are passenger delay and the cost of bus replacement operation. These indicators will enable traffic controllers and train operators to evaluate the efficiency of different predefined solutions and choose the proper one to implement during a disruption.

The remainder of the paper is organised as follows. Sections 2 and 3 describe the framework of the model related to two strategies: short-turning and rail replacement bus operation. Then, section 4 illustrates an application of the proposed model using the case study. Finally, section 5 summarises the paper.

2. Short-Turning Operation Modelling

2.1 Railway network simulation model

This study extends the railway network simulation model by Meesit and Andrews (2018) to include the recoverability analysis capability for a blockage situation. The model by Meesit and Andrews (2018) was constructed using a stochastic-discrete event simulation technique. The framework of this model comprises two main modules: railway network modelling and passenger modelling. The first module simulates the operation of a railway network. The significant characteristics of a railway network, such as track layouts, control systems and operational information (e.g. trains, service routes and timetables) were included. Thus, the detailed schedule of train arrivals and departures at each station, in both normal and disruptive situation can be obtained and used as passenger information in the second module. The second module then imitates passengers using the train services in the network. Three main activities were taken into account: arriving at a station, searching for routes and alighting/boarding a train. A Poisson process was used to model passenger arrivals at a station. Then, an origin-destination matrix was applied to distribute passengers to each destination station. After that the route selection process was started by searching for possible routes to the destinations and selects the best route in terms of the travel time for passengers. Once the second process has finished, passenger objects were created and stored at the station vector based on the station ID waiting for a train to the destination. Then, the alighting and boarding function were finally used to transfer passenger objects between trains and stations when a train stops at a station. These functions are also applied to simulate passengers using bus replacement services in this study.

2.2 Short-turning train services during a blockage situation

Short-turning strategy aims to maintain train services on a part or parts of the disrupted routes. Trains can still be operated to the nearest stations to a disruption and turned around to provide services in the opposite direction of their routes. For unplanned disruptions, this strategy can be modelled by considering the transitions of the timetable during a disruption, which are the transition from the original timetable to the disrupted timetable (Transition 1) and vice versa (Transition 2), see Figure 1.

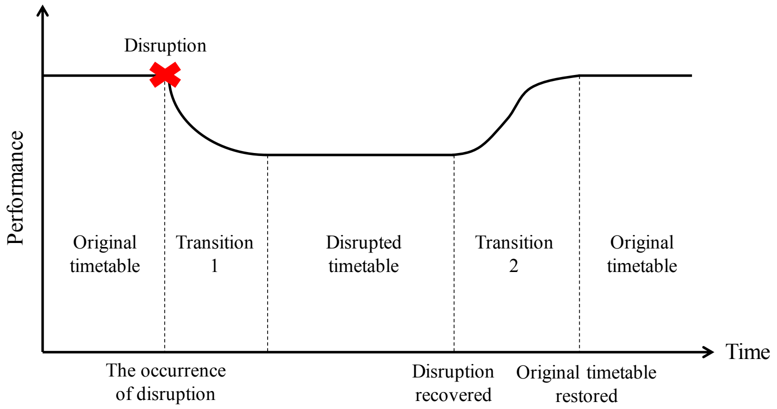


Figure 1. The performance of railway network during a disruption based on Louwerse and Huisman (2014).

Transition 1 happens when a disruption occurs. During this time, some trains on the disrupted route may already begin the service from the terminal station or face the disruption at the middle of the route. Thus, to start the short-turning services, the traffic on the disrupted route needs to be managed. Traffic controllers are required to make a decision on the trains on the network. This study models this circumstance into three main conditions based on the position of the trains on the disrupted route as follows (See Figure 2 as the example).

- If a train is at a terminal station, the model checks whether there is a short-turning station on this section of the route based on the train calling stations. If the condition is true (e.g. T1), the train can continue its service as planned until the short-turning station. Otherwise, the train will be held at the terminal station until the disruption is clear (e.g. T5).
- If a train is at an intermediate station, the model examines that whether the current station is the short-turning station or just a station nearest to the disruption. If the current station is the short-turning station (e.g. T2), the short-turning event is created. The occurrence time of this event will be equal to the next departure time at this station in the opposite direction. However, if the train is delayed, the allowable delay at the turning station (t_{ad}) will be considered for the occurrence time of this event. If the current station is the nearest station to the disruption (e.g. T3 and T6), the model allows traffic controllers to decide whether the train should wait at the station or run back to join the short-turning services at the short-turning station (if applicable) by changing the running back factor (F_{rb}) to *0* or *2* respectively (Figure 2). Nevertheless, if the current station is neither of them (e.g. T7), the train can continue running based on the normal procedure until it arrives the next station. Then, the process is repeated until either of the first two conditions are found.
- If a train is facing the disruption (e.g. T4), traffic controllers can decide whether the train needs to wait, run back to the previous station and wait or run back to the short-turning station and join the short-turning services. These options can also be specified in the model by changing variable F_{rb} to *0*, *1* and *2*, respectively.

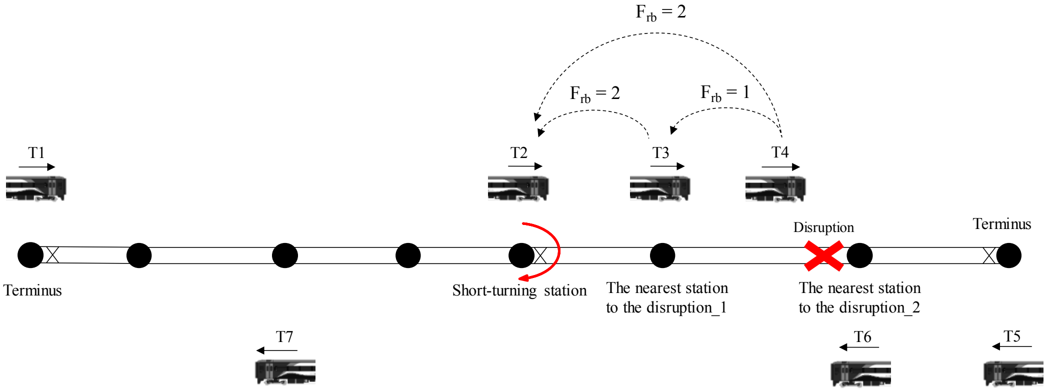


Figure 2. Example of rail traffic on a disrupted route at the beginning of a disruption.

Transition 2 is a state when the disruption is cleared. The trains on the disrupted route that are operating in the short-turning mode need to return to the normal operation. This state therefore requires the decision of traffic controllers, and it probably needs some time to bring the original timetable back to passengers. This study also models this circumstance based on the position of the trains on the disrupted route as described in Transition 1.

- If a train is at a terminal station, the model identifies the suitable departure time for the train based on the original timetable by considering the allowable delay at this terminal station (t_{ad}). The previous departure times that the train could not serve are deleted and counted as cancellations.
- If a train is at an intermediate station, the model investigates whether the current station is a short-turning station. If the condition is true, traffic controllers can decide whether the train needs to wait and continue its service based on the original route or do a short-turn by changing the turning factor (F_{tr}) to *0* and *1,* respectively. However, if the condition is false and the train is a waiting train that is directly impacted by the disruption, the train is authorised to proceed its service immediately once the disruption is cleared.
- Lastly, if a train is facing the disruption, the same process as in the case of a train waiting at an intermediate station is applied.

3. Rail Replacement Bus Operation Modelling

The rail replacement bus service strategy aims to provide an alternative transport option to serve and connect passengers at the impacted stations during a blockage situation. This section presents a rail replacement bus service model that enables train operators to design the bus replacement operation in order to mitigate the impact on stranded passengers. The model is separated into four main events: contacting bus companies, starting a bus service at a disrupted station, stopping a bus at a station and deploying a bus service at a short-turning station.

- The first event happens after the occurrence of a disruption. This event leads buses to be dispatched from the depots to the disrupted stations (See Figure 3). At this point, train operators can decide for the bus routes (i.e. the lists of station stops) and choose the specific stations to start the emergency service. The model will then deploy the bus one by one from the nearest depot to both terminal stations of the designed routes and the selected stations (*SS*), in terms of travel time between depots and stations (t_{dp-i}), based on the number of buses required for the first service in each direction of the route (NB_{f-di}) and the number of buses available at the depot (N_{dp}). Then, the next event "*starting a bus service*" is generated. The occurrence time of this event is equal to simulation time (*Clock*) + organised time (t_{ob}) + travel time (t_{dp-i}). It is noted that during the process, the number of buses available at the nearest depot might not be enough. Thus, when this happens, the buses at the next nearest depot to the station is considered until no more bus is available in the system.
- The second event occurs when a bus has arrived a disrupted station. If the station is a terminal station of a bus route, the bus will run based on the designed route. However, if the station is a specific station, the bus will stop at all stations along the disrupted route based on its direction (*di*). After that the passenger boarding function is called, and the next event "*a bus stops at a station*" is created. The occurrence time of this event is equal to *Clock* + dwell time (t_{bw}) + travel time between stations (t_{o-d}).

- The third event is an event when a bus stops to provide a service at a station. Once it happens, the model investigates whether the current station is an intermediate station, a terminal station with train connections (i.e. a short-turning station) or a terminal station without train connections. If it is an intermediate station, the alighting and boarding function are called in order to transfer passengers. Then, the bus stops at the next station event will be generated as explained in the second event. However, if the current station is a terminal station with train connections, only the alighting function is called because the bus is stored into the Queue waiting for the service when the train arrives. Finally, if the last condition is satisfied, the bus will be turned around to provide the service in the opposite direction. Thus, both alighting and boarding function are called, and the next event will be the bus stops at the next station. The occurrence time of this event is equal to *Clock* + the turnaround time of the bus (t_{bt}).
- The last event occurs when a train arrives a short-turning station. It deploys the buses in the Queue to each route (*br*), that has the current station as a terminal station, based on the number of buses required for the service (NB_{br}). However, if the buses in the Queue are not enough, more buses from the nearest depot are called. The process assumes that these extra buses can be dispatched from the beginning of the disruption. Thus, the travel time of buses from the depot to the disrupted station is not considered again. This event leads the second event to happen at *Clock* + Connection time between trains and buses (t_{cc}).

It is noted that for the passenger simulation, all passengers are modelled to use a normal timetable as travel information. However, once a disruption happens and the mitigation solution is applied, new arrival and existing passengers on the network are assumed to travel based on the disrupted timetable (including both train and bus services). Passengers will reconsider their routes according to the new information. If no route is found or the delay is longer than acceptable, which is based on a Normal distribution (set to μ = 60 minutes, σ = 10 minutes), passengers cancel their journeys. After recovering from a disruption, the normal timetable becomes available again for passengers.

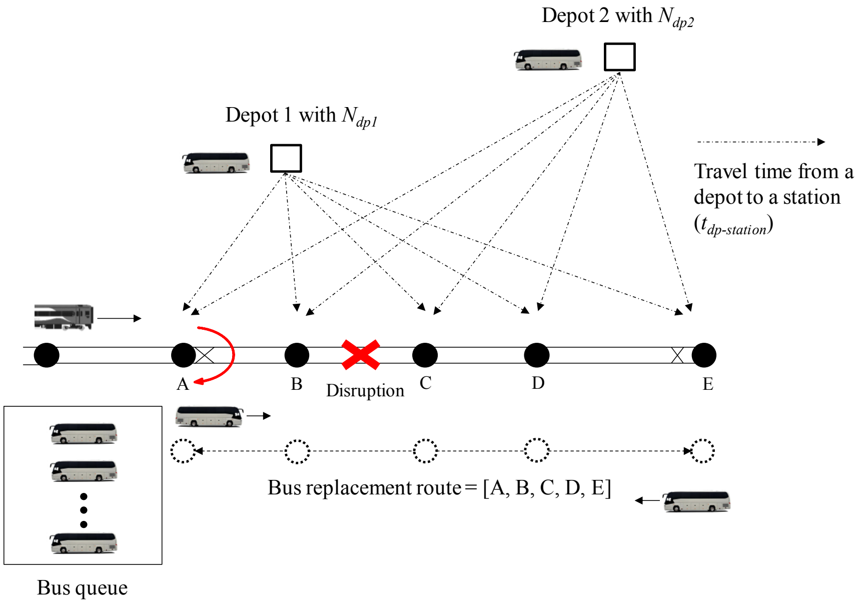

Depot 2 with N_{dp2}
Depot 1 with N_{dp1}
Travel time from a depot to a station ($t_{dp\text{-}station}$)
A
B
Disruption
C
D
E
Bus replacement route = [A, B, C, D, E]
Bus queue

Figure 3. Example of bus replacement operation strategy.

4. Model Application

4.1 Case study

The Liverpool railway network, in the UK is considered as the case study. The network consists of 67 stations. The total length of this network is about 120 km (double track), see Figure 4. There are 7 services operate daily from 6:00 to 24:00. These services are Southport to Hunts Cross (R1), Ormskirk to Liverpool Central (R2) and Kirkby to Liverpool Central (R3), and four loop routes from four terminal stations: Ellesmere Port (R4), Chester (R5), West Kirkby (R6) and New Brighton (R7), via the Liverpool Central station. All trains on the network are the British rail class 507/508 (3 coaches), and they stop at every intermediate station along their routes. For the timetable and passenger data of this network, they were obtained from the study of Meesit and Andrews (2019).

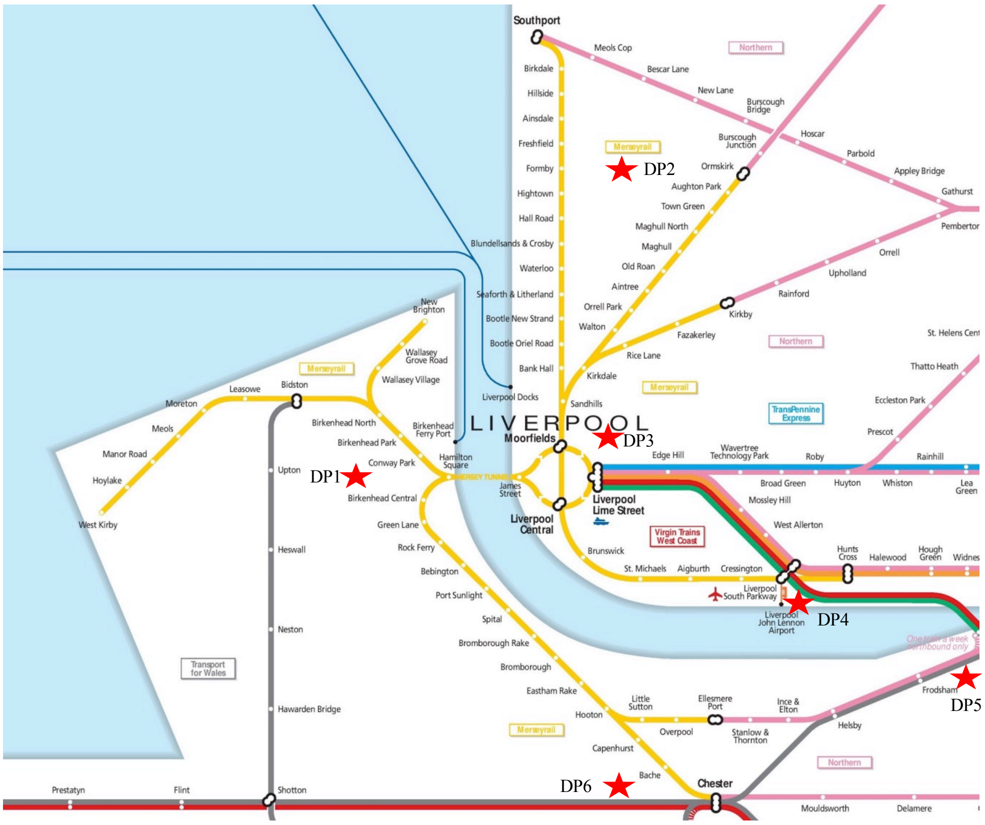


Figure 4. The Liverpool railway network (Merseyrail).

4.2 Key performance indicators

The main goal of implementing a mitigation solution is to reduce the impact of a disruption on passengers. However, in practice, the solution applied is subjected to budget constraint. To this end, this study proposes two performance indicators: total passenger delay (TPD) and operating cost (BOC), to evaluate the efficiency of the potential mitigation solutions as shown in eq. (1) and (2), respectively.

$$\mathrm{TPD} = \mathrm{PC}\cdot\omega + \sum_{\mathrm{p}}^{\mathbf{P}} \mathrm{ADT}_{\mathrm{p}} - \mathrm{PDT}_{\mathrm{p}} \qquad (1)$$

$$\mathrm{BOC} = \sum_{\mathrm{nb}\,=\,1}^{\mathbf{NB}} \mathrm{dt}_{\mathrm{nb}}\cdot\mathrm{fu}_{\mathrm{nb}} + \mathrm{du}_{\mathrm{nb}}\cdot\mathrm{re}_{\mathrm{nb}} \qquad (2)$$

where:

- For eq. (1), PC is the number of passenger journey cancellations, and ω is the delay penalty (set to 60 mins in this study). $\mathrm{ADT}_{\mathrm{p}}$ and $\mathrm{PDT}_{\mathrm{p}}$ are the actual and planned arrival time of a passenger (p) at the destination. It is noted when a disruption occurs, not all passengers will be impacted. Some passengers may obtain a benefit from a delayed train (i.e. catching a delayed train which has not already departed instead of the planned train). Thus, this formula takes both negative and positive effect of the delay into account in order to capture this nature.

- For eq. (2), dt_{nb}, fu_{nb}, du_{nb} and re_{nb} are the bus operating distance, the fuel consumption rate (£0.412/km), the rental duration and the rental cost (including a driver ~£80/hr) of each bus (nb), respectively.

4.3 Model development

The proposed model was developed in C++ 11 environment with Microsoft Visual Studio 2015. Then, the computational experiment was conducted using a computer with a quad core Intel i7 processor CPU 2.60 GHz and 16 GB of RAM running on Window 10, 64-bit. With regard to the stochastic model, the average results from each indicator were predicted from the results of 500 simulations, where the statistics sufficiently converged in about 3 minutes.

4.4 Computational experiment and results

To demonstrate the model, a track blockage disruption is assumed to occur between St Michaels an Aigburth station at 10:00 AM, affecting train services on route R1 (See, Figure 5). The recovery time of this event follows a Normal distribution with mean of 3 hours and 10 minutes standard deviation. To mitigate this situation, traffic controllers and train operators decide to operate the trains on this route in the short-turning mode (using Liverpool central station as the turning station) and provide the bus replacement services to the disconnected stations. Five potential solutions from these strategies are considered as presented in Table I. It is noted that buses are supplied from six main depots within the Liverpool area (see Figure 4), and the number of buses available at each depot (DP1 to DP6) is 10, 8, 15, 12, 5 and 7 respectively. It is assumed the capacity of all buses is 80 seats. Lastly, the shortest distance and the travel time between the disrupted stations, and between the disrupted stations and the depots were acquired from the car-driving option in Google map (2018).

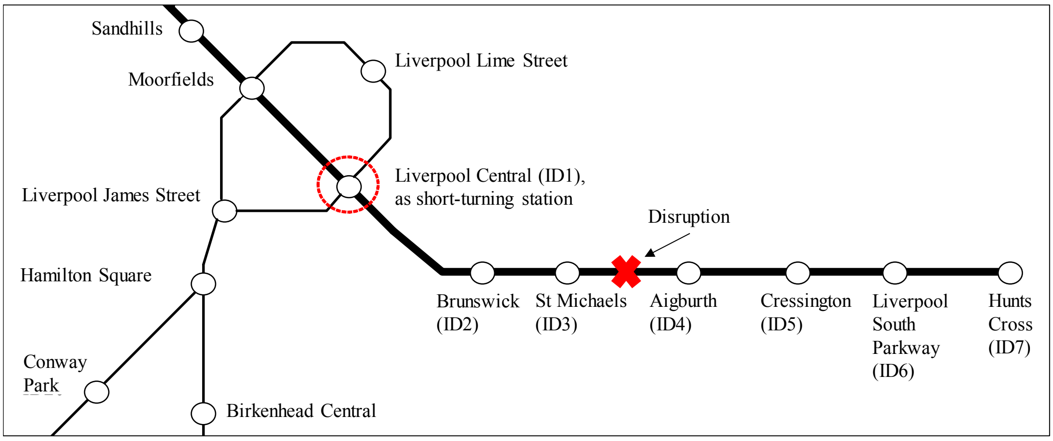


Figure 5. The impacted part of the network in the experiment.

Table I: Example of mitigation solutions considered in the experiment.

Solutions	Short-turning operation				Bus replacement operation (t_{ob}, t_{cc} and t_{bt} = 5 mins)				
	F_{rb} (0, 1 or 2)	F_{tr} (0 or 1)	t_{ad} (at turning station, mins)	t_{ad} (at terminal station, mins)	Bus routes (list of station IDs)	SS (specific stations to begin the emergency service)	$NB_{f\text{-}di}$ (Number of buses for the first service at SSs for each direction)	$NB_{f\text{-}di}$ (Number of buses for the first service at each terminal on each route)	NB_{br} (Number of buses for the consequent services on each route)
S1	Do-nothing solution								
S2	0	0	0	0	-	-	-		-
S3	0	0	10	0	{1, 2, 3, 4, 5, 6, 7}	-	-	{3, 3}	{1}
S4	2	1	10	10	{1, 2, 3, 4, 5, 6, 7}, {1,7}	{4}	{1, 1}	{2, 2}, {1, 1}	{1, 1}
S5	2	0	10	0	{1, 2, 3, 4, 5, 6, 7}, {1, 3, 6, 7}	{3, 6}	{1, 1}, {1, 1}	{2, 2}, {1, 1}	{2, 1}

Table II: Simulation results from each mitigation solution.

Solutions	Passenger delay (mins)	Passenger journey cancellations	TPD (mins)	Bus operating Cost (£)	Number of buses used
S1	29,298	6,961	446,958	0	0
S2	12,394	2,587	167,614	0	0
S3	62,470	580	97,270	2,632	9
S4	63,135	413	87,915	4,177	14
S5	61,429	211	74,089	6,620	22

The simulation results of the potential solutions are presented in Table II. It is obvious that the do-nothing solution was the worst solution in this example. However, for the other solutions, it is difficult to judge which solution is the most suitable countermeasure for this situation. This is because there was the trade-off between two indicators. The higher the operating cost, the smaller the passenger delay (TPD). In this way, traffic controllers and train operators can choose the solution to implement in this scenario based on the budgets and resources they have. For example, if the available budget is £4,500, solution 4 might be feasible to apply. Even though this solution produced 87,915 minutes-delay to passengers, it was still less than that of solutions 2 and 3 about 47.55% and 9.62%.

To implement solution 4, traffic controllers are required to manage the disrupted trains to run backward to join the short-turning operation during the first transition and keep train services in the short-turning mode during the second transition of the timetable. Then, the train operator needs to call 14 buses to operate based on two routes: br_1 = {1, 2, 3, 4, 5, 6, 7} and br_2 = {1, 7}. These buses should be dispatched from depot 3 and 4 to station 1 (9 buses), and 4 (2 buses) and 7 (3 buses), respectively. The detail of this solution can be seen in Table I.

5. Conclusion

A recoverability analysis model for railway networks is presented in this paper. The model is capable of evaluating the efficiency of two mitigation strategies during a track blockage situation: short-turning train services and providing rail replacement bus services. Two performance indicators were proposed: the passenger delay and the operating cost of bus replacement operations. These indicators are beneficial to traffic controllers and train operators to make a decision about the suitable mitigation solution for a particular disruption. In addition, the application of the model was demonstrated using the Liverpool railway network, and the example of the mitigation solution analysis was given in this paper. In the future, the model will be further developed to investigate the optimal solutions for these mitigation strategies. A multi-objective optimisation method, such as a Genetic Algorithm, will be used. Thus, the outcomes of the model will be advantageous to improve the resilience of a railway network during unplanned disruptions.

Acknowledgements

Ratthaphong Meesit is a PhD at the University of Nottingham, who receives a scholarship from the Royal Thai Government. Professor John Andrews is the Royal Academy of Engineering and Network Rail Chair in Infrastructure Asset Management. The authors would like to acknowledge these organisations.

References

Cacchiani, V., Huisman, D., Kidd, M., Kroon, L., Toth, P., Veelenturf, L., and Wagenaar, J. (2014) An overview of recovery models and algorithms for real-time railway rescheduling. *Transportation Research Part B: Methodological*, 63, 15–37.

Cadarso, L., Marín, ángel, and Maróti, G. (2013) Recovery of disruptions in rapid transit networks. *Transportation Research Part E: Logistics and Transportation Review*, 53 (1), 15–33.

Ghaemi, N., Cats, O., and Goverde, R.M.P. (2017) Railway disruption management challenges and possible solution directions. *Public Transport*, 9 (1–2), 343–364.

Ghaemi, N., Cats, O., and Goverde, R.M.P. (2018) Macroscopic multiple-station short-turning model in case of complete railway blockages. *Transportation Research Part C: Emerging Technologies*, 89, 113–132.

Google map (2018) Google map of Liverpool [online].

Gu, W., Yu, J., Ji, Y., Zheng, Y., and Zhang, H.M. (2018) Plan-based flexible bus bridging operation strategy. *Transportation Research Part C: Emerging Technologies*, 91, 209–229.

Jespersen-groth, J., Potthoff, D., Clausen, J., Huisman, D., Kroon, L., Maroti, G., and Nielsen, M. (2009) Disruption management in passenger railway transportation. *In*: *Robust and Online Large-Scale Optimization*. Springer Berlin Heidelberg, 399–421.

Jin, J.G., Teo, K.M., and Odoni, A.R. (2015) Optimizing Bus Bridging Services in Response to Disruptions of Urban Transit Rail Networks. *Transportation Science*, 50 (3), 790–804.

Kepaptsoglou, K. and Karlaftis, M.G. (2009) The bus bridging problem in metro operations: Conceptual framework, models and algorithms. *Public Transport*, 1 (4), 275–297.

Louwerse, I. and Huisman, D. (2014) Adjusting a railway timetable in case of partial or complete blockades. *European Journal of Operational Research*, 235 (3), 583–593.

Meesit, R. and Andrews, J. (2018) Vulnerability assessment modelling for railway networks. *In*: *In: 10th IMA International Conference on Modelling in Industrial Maintenance and Reliability (MIMAR 2018)*. 13-15 June 2018, Manchester, UK., 1–6.

Meesit, R. and Andrews, J. (2019) Ranking the critical sections of railway networks. *The Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit*, To be submitted.

Veelenturf, L.P., Kidd, M.P., Cacchiani, V., Kroon, L.G., and Toth, P. (2015) A railway timetable rescheduling approach for handling large-scale disruptions. *Transportation Science*, 50 (3), 841–862.

Prevention of thermal runaway risk in chemical process industries infrastructure by using model-based fault detection and diagnosis methods

Amine Dakkoune, Lamiae Vernières-Hassimi, Lionel Estel
Normandie Univ, INSA Rouen, UNIROUEN, LSPC, EA4704
685 Avenue de l'Université
76800, Saint Etienne du Rouvray, France

Amine Dakkoune, Dimitri Lefebvre
Normandie Univ, UNILEHAVRE, GREAH
75 rue Bellot
76600, Le Havre, France

Abstract

Protection of critical infrastructures and maintaining of their continuity is a societal obligation aimed to avoid severe socio-economic crises. Among the threats that can affect critical infrastructure are unexpected failures. The chemical industry is among the vital systems that over the past decades, have known serious events affecting lives, facilities and environment, especially when it comes to thermal runaway risk. A method has been developed for early detection and isolation of faults in a chemical reactor based on a reference model. The exothermic reaction of perhydrolysis of formic acid is used as a system test. Based on a kinetic model of the reaction, the method was validated in batch reactor by simulation data in normal and abnormal modes. An experimental validation of this method is now in progress.

This method seeks to improve process resilience in case of runaway event and quickly restores normal operation by preventing the propagation of the event, and therefore contributes to reducing the frequency of threats related to chemical industries, thus ensuring the availability of critical services.

Keywords: Fault detection, fault isolation, critical Infrastructures, chemical processes, thermal runaway.

1. Introduction

Nowadays, critical infrastructures are indispensable in modern society. They provide goods and services that promote the social and economic development of the countries. However, progressive and fast development of socio-economic systems makes their critical infrastructures more complex and therefore vulnerable. This vulnerability can be translated in the case of disruptions or threat by severe socio-economic crises and may endanger the security of the citizen. The chemical industry is one of the vital systems characterized by risky activity [1]. Events in this sector have negative impacts on economic and environmental aspects and may lead to human losses. They cause social panic and even economic crises throughout society. In scientific literature, we found that 25% of chemical events that occurred in France, were caused by thermal runaway reactions [1]. The same percentage was found in another study on thermal runaway events in the United States [2]. Thermal runaway occurs when the heat-flow rate released by the reactions, becomes higher than the heat-flow exchanged with the cooling system of the reactor [3]. As a consequence, thermal runaway can result in an explosion and /or a toxic release that finally may lead to the destruction of the plant and to the formation of secondary fires. In the case of cascading failures, other nearby infrastructures may also suffer from chain interruptions. This phenomenon is called "domino effect". In the history of chemical industries, several catastrophic events were due to thermal runaway, like Seveso (1976) and Bhopal (1984) disasters. The main causes of this dreaded phenomenon were related to the operator errors [1, 4]. Consequently, it has become a major challenge to prevent the events due to thermal runaway, improve the system resilience to different threats and manage efficiently the crisis. This challenge is demonstrated by monitoring chemical reactors carrying out high exothermic reactions. In recent years, the use of fault detection and diagnostic methods in the chemical engineering has experienced continued growth to treat such problem effectively. By looking in the literature, three methods can be distinguished: Quantitative Model Based methods [5, 6] (Observers, EKF, etc.), Qualitative Model Based methods [7] (Fault trees, Digraphs, etc.) and Process History Based methods [8, 9] (Neural Networks, Statistical Classifiers, PCA, etc.).

The purpose of this manuscript is to successfully detect and diagnose failures that occur in chemical industry, in order to avoid their propagation and maintain the sustainability of critical infrastructures. In this purpose, a fault detection and isolation (FDI) method for thermal runaway risk was developed. This approach is based on the reaction model. The reaction of perhydrolysis of formic acid by hydrogen peroxide is used as a test system. The detection method uses a double dynamic threshold for detection of fault and collection of information for diagnosis. Then, the diagnostic method extracts the statistical characteristics of fault and project them in a 2-dimension plan for classification. By using this method, the information extracted will serve as a tool to improve the resilience of the process and to resist accidental disturbances. For example, online control methods [10] allow the process to endure failures, adjust and quickly resume their normal functionality. Moreover, setting up preventive actions and security barriers reduces and / or stops the propagation of the failures when thermal threats occur [11]. The paper is organized as follows: section 2 is dedicated to the reaction model and faults considered. The detection method and the faults isolation method is given in section 3. Simulation and discussion of results were given in section 4. Finally, the conclusion is presented in section 5.

2. Problem Formulation

2.1 Numerical model of the reaction

In this section, a nonlinear model of perhydrolysis reaction of formic acid eq. (1) in a batch reactor is presented [12]. This exothermic reaction characterized by the presence of a reasonable risk for the operators, and it is easy to reproduce in controlled environment.

$$HCOOH + H_2O_2 \rightleftarrows HCOOOH + H_2O \qquad (1)$$

Where, $HCOOH$ is for the formic acid; H_2O_2 for the hydrogen peroxide; $HCOOOH$ for the peroxide formic acid and H_2O for water.

The kinetic expression of this reaction is shown in eq. (2) and Table I:

$$R_{perh} = k_{0,perh}.exp\left(-\frac{E_a}{R}\left(\frac{1}{T}-\frac{1}{T_{ref}}\right)\right).\sqrt{K_{FAD}^{C}\frac{C_{HCOOH}}{C_{H_2O}}}.$$
$$\left(C_{HCOOH}.C_{H_2O_2}-\frac{C_{HCOOOH}.C_{H_2O}}{K^C}\right) \qquad (2)$$

Where, $k_{0,perh}$ is the pre-exponential factor. E_a is the activation energy. R is the gas constant. T is the reaction temperature and T_{ref} is the reference temperature. K_{FAD}^{C} is the association parameter of formic acid and K^C is the equilibrium parameter of the perhydrolysis reaction. C_X represents the concentration of the chemical compound x .

Table I: The values of kinetic and thermodynamic parameters of eq. (2) for T_{ref}=67°C.

Kinetic and thermodynamic parameters	$k_{0,perh}$ $(L.mol^{-1}.s^{-1})$	E_a $(J.mol^{-1})$	ΔH_R $(J.mol^{-1})$
Values	0.15	150000	-5580

The main reaction is characterized by the presence of two parallel secondary reactions eq. (3 and 5). These decompositions reactions increase the heat of the system.
The first decomposition reaction is:

$$HCOOOH \longrightarrow CO_2 + H_2O \qquad (3)$$

The kinetic expression of this reaction is shown in eq. (4) and Table II:

$$R_{decomp1} = k_{0,decomp1}\,.exp\left(-\frac{E_a}{R}\left(\frac{1}{T}-\frac{1}{T_{ref}}\right)\right).C_{HCOOOH} \qquad (4)$$

Table II: The values of kinetic and thermodynamic parameters of eq. (4) for T_{ref}=67°C.

Kinetic and thermodynamic parameters	$k_{0,decomp1}(s^{-1})$	$E_a(J.mol^{-1})$	$\Delta H_R(J.mol^{-1})$
values	0.001	20000	-359000

The second decomposition reaction is:

$$HCOOOH \longrightarrow HCOOH + \frac{1}{2}O_2 \qquad (5)$$

The kinetic expression of this reaction is shown in eq. (6) and Table III:

$$R_{decomp2} = k_{0,decomp2}\,.exp\left(-\frac{E_a}{R}\left(\frac{1}{T}-\frac{1}{T_{ref}}\right)\right).[C_{HCOOOH}] \qquad (6)$$

Table III: The values of kinetic and thermodynamic parameters of eq. (6) for T_{ref}=67°C.

Kinetic and thermodynamic parameters	$k_{0,decomp2}$ (s^{-1})	E_a $(J.mol^{-1})$	ΔH_R $(J.mol^{-1})$
values	0.0009	20200	-163000

Besides, the hydrogen peroxide used in the reaction can also decompose eq. (7). In this case, the reaction system becomes dangerous [13].

$$H_2O_2 \longrightarrow H_2O + \frac{1}{2}O_2 \tag{7}$$

Hydrogen peroxide can decompose in two ways:

1. In the case of spontaneous decomposition under the effect of temperature, the kinetic expression of reaction eq. (7) is shown in eq. (8) and Table IV.

$$R_{spont} = k_{0,spont}\,.exp\left(-\frac{E_a}{R}\left(\frac{1}{T}-\frac{1}{T_{ref}}\right)\right).C_{H_2O} \tag{8}$$

Table IV: The values of kinetic and thermodynamic parameters of eq. (8) for T_{ref}=140°C.

Kinetic and thermodynamic parameters	$k_{0,spont}$ (s^{-1})	E_a $(J.mol^{-1})$	ΔH_R $(J.mol^{-1})$
values	0.0000924	150000	-98000

2. In the case of decomposition by copper sulfate as impurity, the kinetic expression of reaction eq. (7) is shown in eq. (9) and Table V.

$$R_{decomp3} = R_{spont} + R_{catal.Cu(II)} \tag{9}$$

With:

$$R_{catal.Cu(II)} = 2k_{0,A}.exp\left(-\frac{E_{a,A}}{R}\left(\frac{1}{T}-\frac{1}{T_{ref}}\right)\right).[C_{Cu^{2+}}].\left[C_{H_2O_2}\right]^2 + \\ 2k_{0,B}.exp\left(-\frac{E_{a,B}}{R}\left(\frac{1}{T}-\frac{1}{T_{ref}}\right)\right).\left[C_{H_2O_2}\right].\sqrt{[C_{Cu^{2+}}]} \tag{10}$$

Table V: The values of kinetic and thermodynamic parameters of eq. (10) for T_{ref}=140°C.

Kinetic and thermodynamic parameters	$k_{0,A}$ $(L^2.mol^{-2}.s^{-1})$	$E_{a,A}$ $(J.mol^{-1})$	$k_{0,B}$ $(L^2.mol^{-2}.s^{-}$	$E_{a,B}$ $(J.mol^{-1})$	ΔH_R $(J.mol^{-1})$
values	0.0163	162000	0.0035	69700	-93200

The material balances for formic acid, hydrogen peroxide, peroxyformic acid and water in batch reactor are represented by the differential equations eq. (11).

$$\frac{d}{dt}C_{HCOOH} = -R_{perh} + R_{decomp2}\ ; \qquad \frac{d}{dt}C_{HCOOOH} = R_{perh} - R_{decomp1} - R_{decomp2} \tag{11.a}$$

$$\frac{d}{dt}C_{H_2O_2} = -R_{perh} - R_{decomp3}\ ; \qquad \frac{d}{dt}C_{H_2O} = R_{perh} + R_{decomp1} + R_{decomp3} \tag{11.b}$$

The energy balance in the batch reactor for the reaction mixture is expressed by the differential equations shown in eq. (12):

$$\frac{d}{dt}T_R = \frac{1}{\sum m_R c_{p_R}}\left(U.A.\left(T_j - T_R\right) - \left(\sum R_R.\Delta H_R.V_R\right) - q_{loss}\right) \tag{12}$$

Where m_R is the initial mass of the reaction mixture. C_{P_R} is the reaction heat capacity of the reaction mixture. U is the overall heat-transfer coefficient. A is the heat transfer area. T_j is the heat carrier temperature circulating in the reactor jacket. R_R is the reaction rate. ΔH_R is the enthalpy of reaction. V_R is the volume of the reaction mixture. q_{loss} is the heat loss due to evaporation.

2.2 Normal operating conditions

A numerical model of the reaction of perhydrolysis of formic acid is represented in Figure 1. This model is obtained in normal operating conditions shown in Table VI. Figure 1 represents also the experimental measurements of the temperature variations of the same reaction. By comparing the theses temperature profiles, a good agreement between the numerical and the experimental measurements temperatures can easily be observed, therefore the model is able to follow correctly the thermal behavior of the reaction, especially between the beginning of the reaction and when the reaction exceeds its maximum temperature. The maximum temperature is an important parameter that is taken into account as a safety tool to study thermal risks [14].

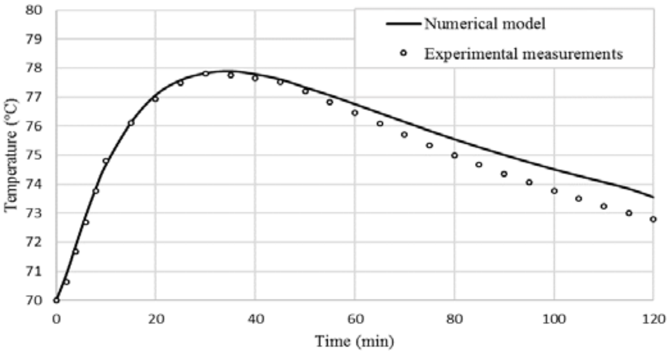


Figure 1. Numerical model and experimental measurements of the temperature reaction of perhydrolysis of acid formic in function of time (min).

Table VI: Normal operating conditions.

Parameters of system	Sample volume	Initial conc. of formic acid	Initial conc. of hydrogen peroxide	Initial temperature of reaction	Jacket temperature
Symbol	V_R	FA	HP	T_R	T_j
Values	1.2 L	2.5 mol.L^{-1}	2.8 mol.L^{-1}	70°C	70°C

2.3 Description of the major faults

Several causes may lead to a thermal runaway event. The most probable causes have been due to operator errors according to studies carried out in France [15] and United Kingdom [4]. The operator errors considered in this paper have been described as follow:

- Modification of initial concentrations of reactants (formic acid FA and hydrogen peroxide HP) due to errors in the preparation step.
- Presence of impurities (copper sulfate Cu) due to insufficient cleaning of the reactor.
- Increase of the temperature (T_j) of the cooling jacket due to non-respect of procedures.

The reaction system becomes more dangerous when normal operating conditions are exceeded because of such errors. These errors can change de reaction model and the thermal behaviour of the system. The behavior is considered abnormal if the maximal temperature of reaction reaches 79 °C.

3. The FDI method

3.1 Faults detection

Fault detection is an effective method to alert and inform the operator of the existence of faults in the system. An early detection lets the time to operator to react before that the fault becomes uncontrollable. In this context, a method of early detection of faults based on the use of a double dynamic threshold has been developed in our previous works [15, 16], and shows an early detection of faults in the detection performance test. This detection method was improved in this paper by taking into account another fault type. The thresholds define dynamic tolerance ranges and it is calculated according to three principles:

1. An increase of initial concentration of the reagents (FA and HP) and the presence of an impurity (Cu) in the reaction mixture cause a rise in the maximum temperature of the reaction above 79°C.
2. A temperature marge of tolerance $M_T = 0.1°C$ is considered in order to avoid false alarms due to sensor errors.
3. Only single faults are considered.

The first threshold is used for the early detection of faults ($D_{limit}(t)$) eq. (14), it represents the profile of the reaction temperature that does not exceed 79°C. While the second threshold is used to perform the classification of these detected faults ($S_{limit}(t)$) eq. (15), and it represents the profile of the reaction temperature that does not exceed 80°C.

$$D_{Limit}(t)=\max(\min(T_{FA1}(t),T_{HP1}(t),T_{Cu1}(t), T_{Tj1}(t)), T_{Nominal}(t)+M_T) \quad (14)$$

$$S_{Limit}(t)=\max(\min(T_{FA2}(t),T_{HP2}(t),T_{Cu2}(t), T_{Tj2}(t)), T_{Nominal}(t)+5.M_T) \quad (15)$$

Where $T_{Nominal}(t)$ is the reaction temperature profile for the nominal conditions. Tx(t) represents the temperature reaction profile that does not exceed 79°C or 80°C for the maximal acceptable value of (x) shown in Table VII.

Table VII: Maximal acceptable values of FA, HP, Cu and T_j for $D_{limit}(t)$ and $S_{limit}(t)$.

	Maximal acceptable value of (x)			
x	FA (mol.L^{-1})	HP (mol.L^{-1})	Cu (mol.L^{-1})	T_j (°C)
$D_{Limit}(t)$	2.74	3.06	0.02	70.8
$S_{Limit}(t)$	2.96	3.33	0.08	71.7

The definition of $D_{Limit}(t)$ and $S_{Limit}(t)$ in eq. (14 and 15) aims to avoid non-detections and false alarms (Figure 2) as follows:

- The use of the “min” operator reduces the rate of non-detection: the dynamic tolerance range is constrained at each point t by the minimal value of $T_{FA1}(t)$, $T_{HP1}(t)$, or $T_{Cu1}(t)$ in eq. (14) and $T_{FA2}(t)$, $T_{HP2}(t)$, or $T_{Cu2}(t)$ in eq. (15).
- The use of the “max“ operator with the nominal temperature $T_{Nominal}(t)$ plus temperature marge of tolerance M_T reduces the rate of false alarms. Note that this condition also delays the detection.

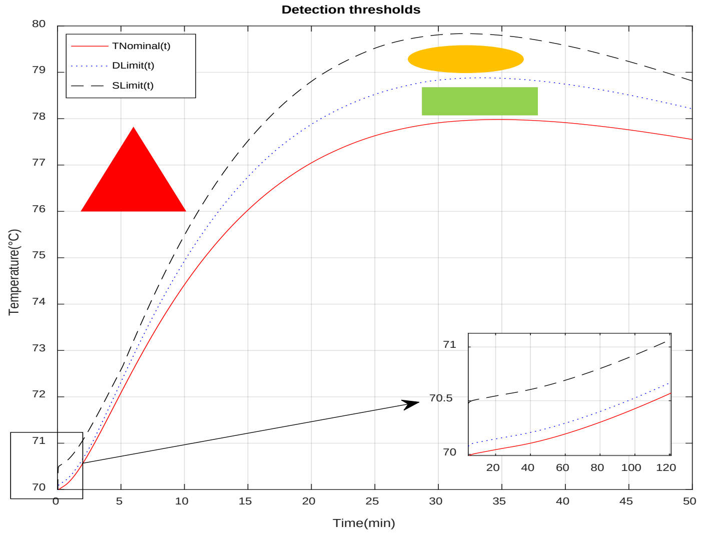


Figure 2. Dynamical thresholds $S_{Limit}(t)$and $D_{Limit}(t)$ compared to $T_{Nominal}(t)$.

The Figure 2 shows three safeties modes of reaction according to threshold type:

- The reaction is in a safe mode when the reaction temperature is below the first threshold $D_{Limit}(t)$ (green rectangle area).
- The reaction is in a dangerous mode but still acceptable when the reaction temperature is between $D_{Limit}(t)$ and $S_{Limit}(t)$ (orange circle area).
- The reaction is in an unacceptable mode when the reaction temperature is above $S_{Limit}(t)$ (red triangle area).

The detection is performed by comparing the temperature measurements with the first dynamics thresholds $D_{Limit}(t)$. Because of the noise, the measured temperature is filtered f(T) by using an Extended Kalman Filter (EKF). The decision function of faults D(t) is defined as follows eq. (16):

$$D(t) = 1 \text{ if } f(T(k)) > D_{Limit}(k) \text{ for } k \in \{t\text{-}n+1,\dots t\text{-}1,t\} \qquad (16)$$
$$D(t) = 0 \text{ otherwise.}$$

A fault is detected, if the measured temperature profile exceeded the first threshold $D_{Limit}(t)$ for n=10 successive points of the measured temperature $k \in \{t\text{-}n+1,\dots t\text{-}1,t\}$, this condition limits isolated false alarms. Figure 3 shows an example of fault detection in the considered reaction due to an increase of the initial concentration of hydrogen peroxide (HP).

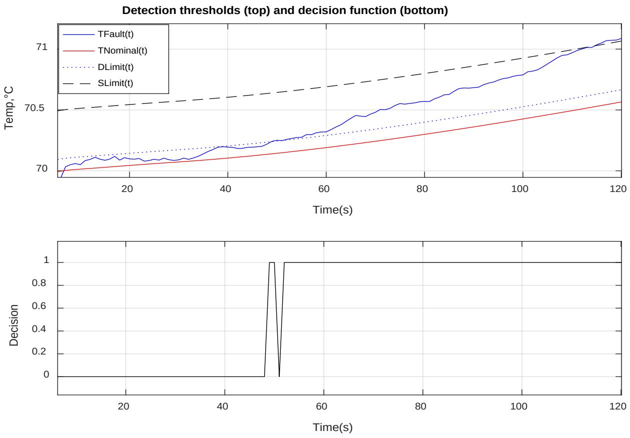


Figure 3. Example of the considered reaction with a fault in the initial concentration of HP and the decision function.

3.2 Faults isolation

Faults isolation consists of establishing a diagnosis by isolating the most probable candidate fault among a set of faults candidates. It is carried out as follows:

During the reaction phase, when the detection method described above sends an alert indicating the detection of a fault, a time windows is used to continues to collect more temperature measurements (N) in the dangerous area W = {T(p), T(p+1), … T(p+K)}. Where p and K are the position and the size of the window W respectively (Figure 4). These measurements will be used to complete the diagnostic task. The recording stops when the temperature measurements exceeded the second threshold $S_{Limit}(t)$. The necessity of additional temperature measures appears through the insufficient measurements collected in the detection phase. These not enough measures do not allow separating the various classes of faults because during the first seconds of the reaction the faults behaviors are very similar.

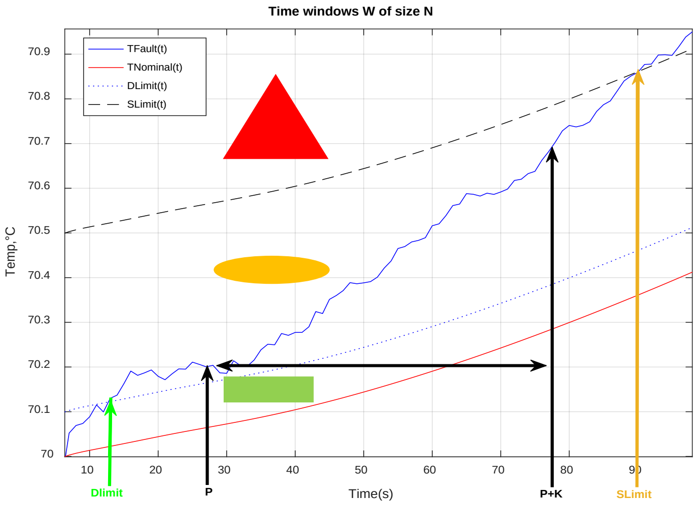


Figure 4. Data collection for diagnosis issues.

The temperature measurements collected and projected in the window W, are studied and classified according to several statistical characteristics like the average value, the variance, the covariance, the mode, the median, the skewness, the kurtosis, etc. of the temperature. According to several tests, the variance and skewness of the temperature shows a good separation between the different classes of faults (Figure 5).

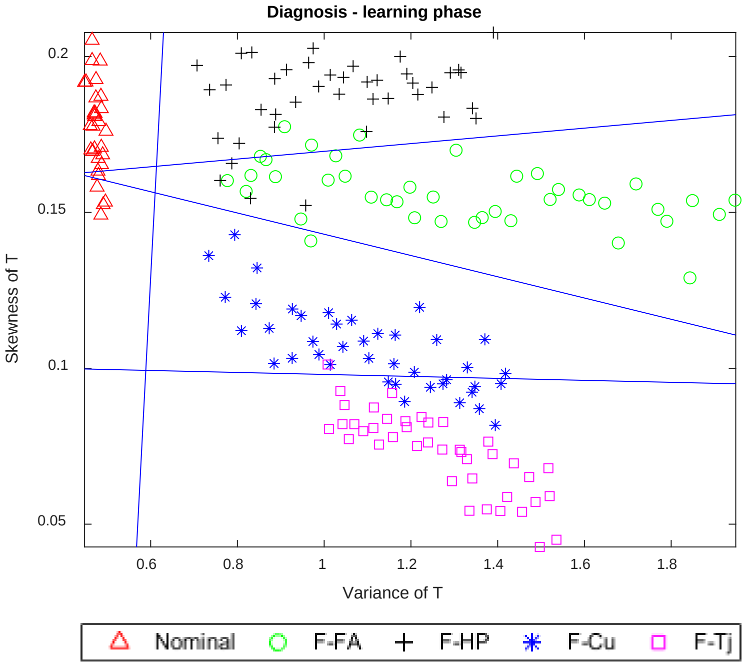


Figure 5. Fault (F) diagnosis by means of classification in window W = [30s 330s].

4. Results and Discussion

In order to validate the FDI method proposed, a set of 100 simulations are emulated. These simulations contain initial and random faults including normal behavior of the reaction. In order to consider the measurement errors, a noise of magnitude 0.1°C consistent with experimental conditions usually adopted with the considered reaction was added. The parameters used to achieve the FDI method are presented in Table VIII.

Table VIII: Parameters of the FDI method.

FDI parameters	**Values**
Sampling period	1s
Temperature marge of tolerance M_T	0.1°C
Memory parameter n to avoid false alarms	10
Position p of the time window for diagnosis	30s
Size K of the time window for diagnosis	330s

Delays in fault detection for 100 random simulations are represented in Figure 6. The results shows an early detection of these faults. The detection delay does not exceed 2 minutes: All faults are detected between 20s and 120s. For that, the mean detection delay is 52s. The false alarm rate is 0% and the detection rate is 100%.

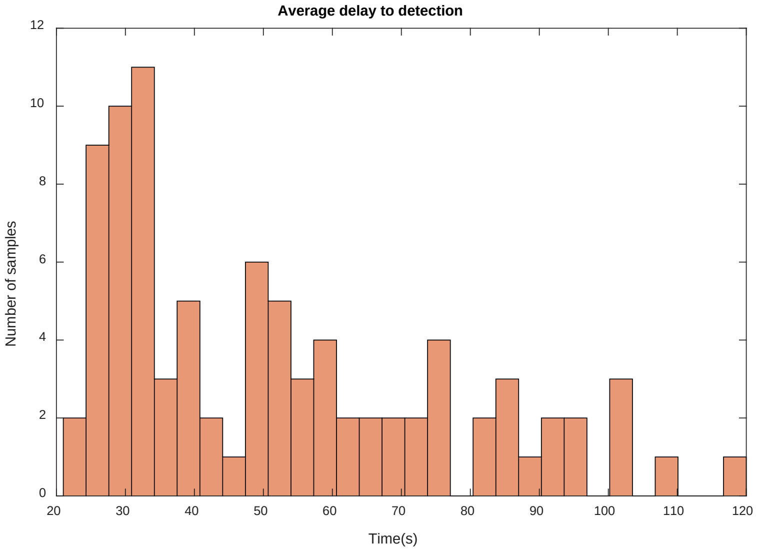


Figure 6. Distribution of the delays to the detection of the 100 random simulations

The results of faults classification are provided in the window of classification in Figure 7 and in the confusion matrix in Table IX.

The matrix details the results presented in the Figure 9, it provides for each class of fault the classification performance. The groups (FA, HP) = 4% and (Cu, T_j) = 14% show that for 4% (resp. 14%) of the patterns with a fault of class FA (resp. Cu), a wrong decision HP (resp. T_j) is returned. One the average, good results are obtained for classification, except some measures of FA and Cu faults.

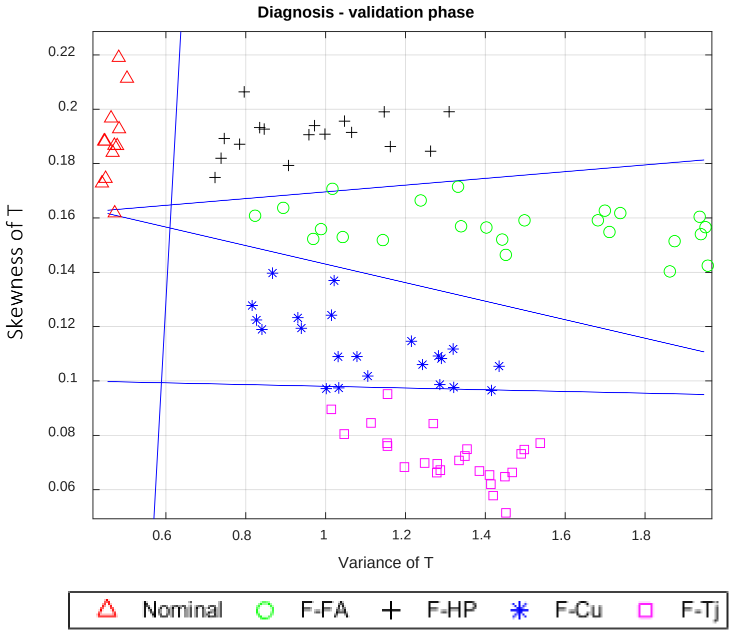


Figure 7. Fault (F) classification for the 100 random simulations in W = [30s 330s].

Table IX: Performance of the diagnosis (confusion matrix).

	Nominal	FA	HP	Cu	T_j
Nominal	100%	0%	0%	0%	0%
FA	0%	96%	4%	0%	0%
HP	0%	0%	100%	0%	0%
Cu	0%	0%	0%	86%	14%
T_j	0%	0%	0%	0%	100%

5. Conclusion

An FDI method has been developed to prevent thermal runaway risk in chemical reactors, by using a double dynamic threshold for fault detection, and the extraction of the statistical characteristics of fault cause for isolation. The proposed method used a reaction model in a batch reactor. The simulations results show an early detection of the faults with an average delay of 52 seconds. This detection delay is widely enough to control the reaction temperature and resume functionality as quickly as possible by, for example, injecting the solvent or by increasing the temperature of the cooling system (this delay is small compared to the time required to reach the maximal temperature of 80°C that is about 30 minutes). The analysis of the detection performance shows that all fault simulations are detected and no false alarms were found. The isolation method provides also a good result despite some wrong decision of FA and Cu faults due to the similarity of their behaviors with HP and T_j respectively. The future works are to confirm the proposed method by experimental tests and to provide suitable information to choose the most adapted control method for each detected faults.

Acknowledgements

This project AMED has been funded with the support from the European Union with the European Regional Development Fund (ERDF) and from the Regional Council of Normandie.

References

[1] Dakkoune, A., Vernières-Hassimi, L., Leveneur, S., Lefebvre, D.and Estel, L. (2018). Risk analysis of French chemical industry. *Saf. Sci*. 105, 77–85.

[2] Balasubramanian, S.G and Louvar, J.F. (2002). Study of major accidents and lessons learned. *Process Saf. Prog*. 21, 237–244.

[3] Jiang, J., Jiang, J., Wang, Z. and Pan, Y. (2016). Thermal runaway criterion for chemical reaction systems: A modified divergence method. *J. Loss Prev. Process Ind*. 40, 199–206.

[4] Saada, R., Patel, D. and Saha, B. (2015) Causes and consequences of thermal runaway incidents—Will they ever be avoided? *Process Saf. Environ. Prot*. 97, 109–115.

[5] Pierri, F., Paviglianiti, G., Caccavale, F. and Mattei, M. (2008) Observer-based sensor fault detection and isolation for chemical batch reactors. Engineering Applications of Artificial Intelligence 21, 1204–1216.

[6] Benkouider, A.M., Buvat, J.C., Cosmao, J.M. and Saboni, A. (2009) Fault detection in semi-batch reactor using the EKF and statistical method. *Journal of Loss Prevention in the Process Industries*. 22, 153–161.

[7] Ulerich, N. H., and Powers G. J. (1988) « On-line hazard aversion and fault diagnosis in chemical processes: the digraph+fault-tree method », *IEEE Transactions on Reliability*, vol. 37, no 2, p. 171‑ 177.

[8] Choi, S.W., Lee, C., Lee, J.-M., Park, J.H. and Lee, I.-B. (2005) Fault detection and identification of nonlinear processes based on kernel PCA. *Chemometrics and Intelligent Laboratory Systems.* 75, 55–67.

[9] Zhang, J. (2008). Batch-to-batch optimal control of a batch polymerisation process based on stacked neural network models. *Chemical Engineering Science, Control of Particulate Processes*. 63, 1273–1281.

[10] Vernières-Hassimi, L., and Leveneur, S. (2015). Alternative method to prevent thermal runaway in case of error on operating conditions continuous reactor, *Process Safety and Environmental Protection*, vol. 98, p. 365‑ 373.

[11] Misuri, A., Khakzad, N., Reniers, G., Cozzani, V. (2018). A Bayesian network methodology for optimal security management of critical infrastructures. *Reliability Engineering & System Safety*. In Press, Corrected Proof.

[12] Zheng, J.L., Wärnå, J., Salmi, T., Burel, F., Taouk, B. and Leveneur, S. (2016) Kinetic modeling strategy for an exothermic multiphase reactor system: Application to vegetable oils epoxidation using Prileschajew method. *AIChE J*. 62, 726–741.

[13] Vernières-Hassimi, L., Dakkoune, A., Abdelouahed, L., Estel, L. and Leveneur, S. (2017). Zero-Order Versus Intrinsic Kinetics for the Determination of the Time to Maximum Rate under Adiabatic Conditions TMRad Application to the Decomposition of Hydrogen Peroxide. *Ind. Eng. Chem. Res*. 56, 13040–13049.

[14] Vernières-Hassimi, L., Seguin, D., Abdelghani-Idrissi, M.A. and Mouhab, N. (2014). Estimation and localization of maximum temperature in a tubular chemical reactor by luenberger state observer. *Chem. Eng. Commun*. 202, pp. 70-77.

[15] Dakkoune A., Vernières-Hassimi L. Leveneur S., Lefebvre D. and Estel L. (2018) Fault Detection in the Green Chemical Process: Application to an Exothermic Reaction, *Chemical Engineering Transactions*, Vol. 67, 43-48.

[16] Dakkoune A., Vernières-Hassimi L. Leveneur S., Lefebvre D. and Estel L. (2018) « Model-based fault detection and isolation for chemical processes: Application to the prevention of thermal runaway », *in 2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, p. 1352‑ 1358.

Time Series Segmentation of Linear Stochastic Processes for Anomaly Detection Problem Using Supervised Methods

Dmitry Efrosinin
Institute for Stochastics, Johannes Kepler University
Altenbergerstrasse 66
4040, Linz, Austria

Valentin Sturm
Linz Center of Mechatronics GmbH
Altenbergerstrasse 66
4040, Linz, Austria

Abstract

The problem of time series segmentation for real-world applications has received much attention recently. Different industrial machines as elements of critical infrastructure for energy extraction, pumping, generation and other operations are equipped by hundreds of sensors which measure and evaluate variety data sets such as temperature, vibration, accelerations, pressure, voltage and so on. In many cases these measurements are unreliable, incomplete, inconsistent, and noisy and hence they can be interpreted as realizations of some linear stochastic processes. The task of recognizing of anomalous operation mode of machines can be reduced to the problem of pattern recognition, change point detection or segmentation in time series. In this paper we propose a general approach for time series segmentation of linear stochastic processes based on supervised learning algorithms which are machine learning algorithms using a mapping from input samples to a target attribute of the data. We also perform empirical examples for some hypothetical time series segmentation.

Keywords: Time series segmentation, anomaly detection, supervised methods, machine learning algorithms.

1. Introduction

The task of time series segmentation is becoming increasingly popular in various fields including medicine, aerospace, and finance, human and animal activity recognition as well as for anomaly detection by operation of industrial systems, equipment and machines. as part of critical infrastructure. Time series data represents time ordered sequences of measurements reflecting the behavior of systems. These behaviors can change over time due to some systematic and random internal or external events. Time series segmentation [8] is based on finding the abrupt changes in data when different statistical properties of the time series change. These changes can reflect the possible future failures and confirm unexpected behavior of some technical system. Such problem of pattern recognition in time series generated by sensors is known as anomaly detection problem [5]. The proper handling of equipment and machines as well as timely preventive maintenance based on measurements generated by sensors allow to avoid failures in critical infrastructure which as a result can have dramatic economic, social and environmental consequences. As an example of such disastrous effect of a technical failure is a Sayano-Shushenskaya power station accident in 2009. The high vibration of the bearing in one of the turbine leads to destruction of the turbine cover and as a result the turbine hall and engine room were flooded. Significant portion of supply to the local electric grid was lost. This accident has shown a necessity to use modern sensors for generating data sets about state and operational mode of equipment as well as to develop appropriate methods needed to classify these data samples with the aim to predict possible anomalies.

The sensor data is normally noisy and have outliers. In many cases it can be treated as realization of some linear stochastic process. Anomaly detection problem reduces then to a segmentation problem or to the change point detection problem in a time series. Additionally it should be taken into account that machines can have different operational profiles, for example variable intensities, modes and so on. Hence the problem of multiple segments identification must be solved in this case. Many machine learning algorithms have been developed and implemented for change point detection. A variety of supervised classifiers can be used for learning problem in a context of anomaly identification, time series segmentation and change point detection. These methods can be divided into two groups: binary class classifiers and multi-class classifiers. The first group includes such methods as support vector machine (SVM) [2], Naïve Bayes [11], Logistic Regression [3]. In multi-class case the following methods can be used: Decision tree [13], Neares Neighbor [10], SVM [7], Naïve Bayes, Bayesian Net [9], Hidden Markov Model (HMM) [14], Conditional Random Field (CRF) [1], Gaussian Mixture Model (GMM) [12].

In this paper we examine for a change point detection problem a general methods including supervised learning algorithms that learn to map from input data and appropriate derived features to a target attribute of the data which will be specified as a segment or class label.

2. Definitions

2.1 Stochastic processes

Assume that a time series data stream is a finite sequence of elements

$$\{x_1, \dots, x_n\},$$

which is a realization of some linear stochastic process $\aleph = \{X_t\}_{t \in \mathbb{N}_0}$. A time series calls stationary if the corresponding stochastic process has finite variance and constant values of the moments over time. Denote by

$$Z_t \sim N(0, \sigma^2)$$

is a normal distributed white noise process. We want to define three different types of linear stochastic processes:

1. **AR(p)-Processes**: A process $\aleph = \{X_t\}_{t \in \mathbb{N}_0, t \geq p}$ is called an AR(p)-Process (Autoregressive) if it fulfils the following equation [4]:

$$X_t - \varphi_1 X_{t-1} - \cdots - \varphi_p X_{t-p} = Z_t.$$

2. **ARMA(p,q)-Processes**: A process $\aleph = \{X_t\}_{t \in \mathbb{N}_0, t \geq \max\{p,q\}}$ is called an ARMA(p,q)-Process (Autoregressive-Moving-Average) if it fulfils the following equation [4]:

$$X_t - \varphi_1 X_{t-1} - \cdots - \varphi_p X_{t-p} = Z_t - \theta_1 Z_{t-1} - \cdots - \theta_q Z_{t-q}.$$

3. **ARCH(p)-Processes:** A process $\aleph = \{X_t\}_{t \in \mathbb{N}_0, t \geq p}$ is called an ARCH(p)-Process (Autoregressive Conditional Heteroskedasticity) if it fulfils the following equations [6]:

$$X_t = \sigma_t Z_t$$
$$\sigma_t^2 = a_0 + a_1 X_{t-1}^2 + \cdots + a_p X_{t-p}^2.$$

A change point is a point between different states of a stochastic process which generates the time series data sets with corresponding segments. Change point detection can be defined a statistical problem of hypothesis testing, where the null hypothesis $\boldsymbol{\mathcal{H}_0}$ means that no change occurs while the alternative one $\boldsymbol{\mathcal{H}_1}$ stands for a change point, i.e.

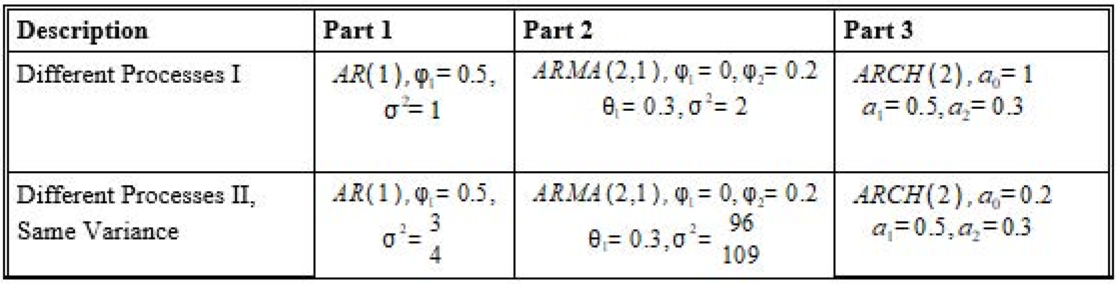
$$\boldsymbol{\mathcal{H}_0}: \mathbb{P}_{X_0} = \cdots = \mathbb{P}_{X_k} = \cdots = \mathbb{P}_{X_n},$$
$$\boldsymbol{\mathcal{H}_1}: \exists\, k^* \in (0, n): \mathbb{P}_{X_0} = \cdots = \mathbb{P}_{X_{k^*}} \neq \mathbb{P}_{X_{k+1^*}} = \cdots = \mathbb{P}_{X_n},$$

where $\mathbb{P}_{X_i}$ is a probability density function of time series starting at point x_i and k^* is a change point.

2.2 Experimental set-up

We construct 4 different scenarios, in every scenario we have 10000 samples of three different states each, where the underlying processes of the different states have the form as described in Table 1

Table I: Short description of the 4 different considered cases with specification of the underlying processes of each of the three occurring segment



Description	Part 1	Part 2	Part 3
Different Processes I	$AR(1), \varphi_1 = 0.5,$ $\sigma^2 = 1$	$ARMA(2,1), \varphi_1 = 0, \varphi_2 = 0.2$ $\theta_1 = 0.3, \sigma^2 = 2$	$ARCH(2), a_0 = 1$ $a_1 = 0.5, a_2 = 0.3$
Different Processes II, Same Variance	$AR(1), \varphi_1 = 0.5,$ $\sigma^2 = \frac{3}{4}$	$ARMA(2,1), \varphi_1 = 0, \varphi_2 = 0.2$ $\theta_1 = 0.3, \sigma^2 = \frac{96}{109}$	$ARCH(2), a_0 = 0.2$ $a_1 = 0.5, a_2 = 0.3$

Same Variance, Different Autocorrelation	$AR(1), \varphi_1 = 0.5,$ $\sigma^2 = \frac{4}{3}$	$AR(1), \varphi_1 = 0.8,$ $\sigma^2 = \frac{9}{25}$	$AR(1), \varphi_1 = -0.5,$ $\sigma^2 = \frac{4}{3}$
Different Variance, Same Autocorrelation	$AR(1), \varphi_1 = 0.5,$ $\sigma^2 = 1$	$AR(1), \varphi_1 = 0.5,$ $\sigma^2 = 2$	$AR(1), \varphi_1 = 0.5,$ $\sigma^2 = 3$

In Figure 1-4 we can see a realization of our different scenarios 1, where the vertical dotted lines mark the points where the underlying processes change. Different segments are easy to distinguish visually:

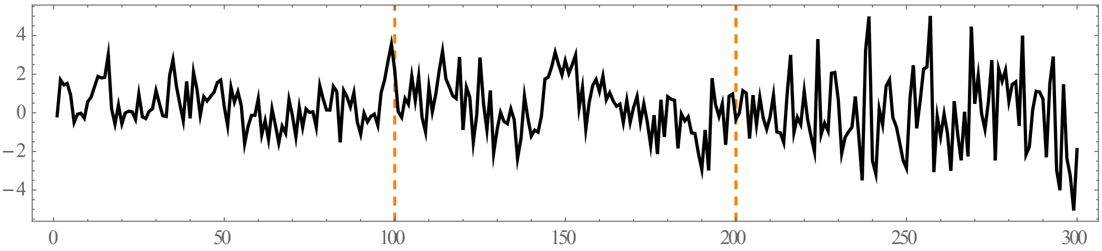


Figure 1. Depiction of a realization using the processes from experimental setup 1.

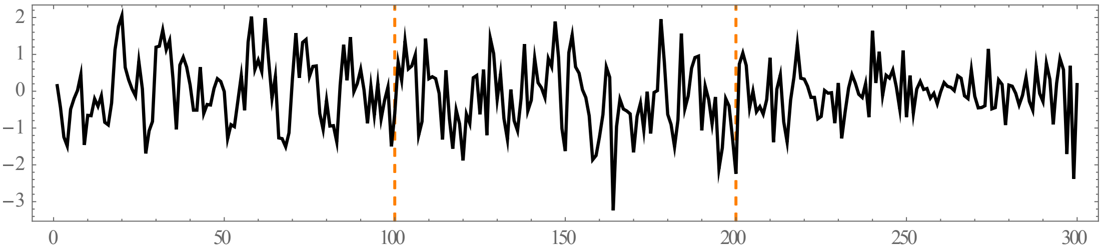


Figure 2. Depiction of a realization using the processes from experimental setup 2.

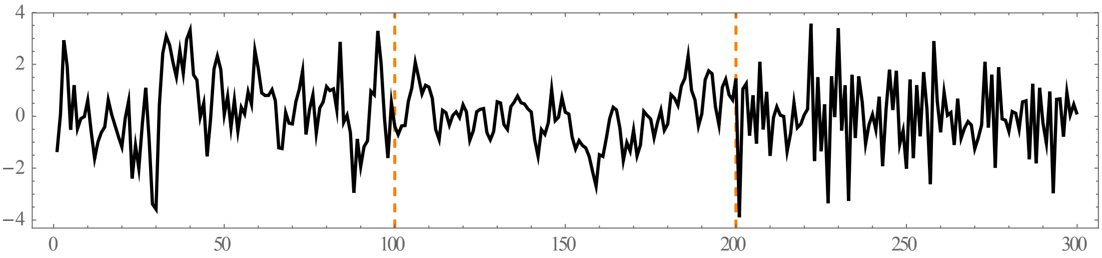


Figure 3. Depiction of a realization using the processes from experimental setup 3.

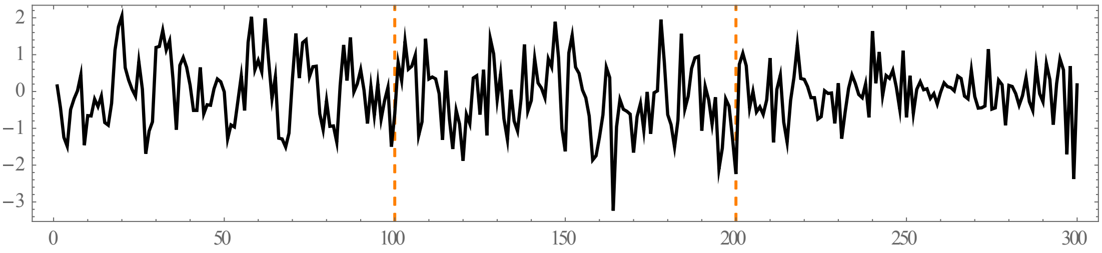


Figure 4. Depiction of a realization using the processes from experimental setup 4.

2.3 Performance metrics

To estimate the quality of time series segmentation we use a number of performance metrics describing in the context of binary classification. The problem can be extended to classification of a greater number of classes by providing the measures for each class independently or in combination. In our special case we assume three classes and hence we calculate the following measures by merging two classes, such that only two classes remain. This procedure will be repeated for all possible combinations. Accuracy is calculated as the ratio of correctly classified data points to a total data points which can be ineffective for performance evaluation in a class-imbalanced dataset,

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+FN+TN}. \tag{1}$$

Sensitivity or Recall is defined as the proportion of a class of interest, e.g. where change point between segments occurs, that was recognized correctly,

$$\text{Sensitivity} = \text{Recall} = \frac{TP}{TP+FN}. \tag{2}$$

For imbalanced class distribution where the ratio of changes to total data is small one can use g-mean, which utilizes both the ratio of positive accuracy (Sensitivity) and the ratio of negative accuracy,

$$G - mean = \sqrt{\text{Sensitivity} \cdot \text{Specificity}}, \tag{3}$$

where

$$\text{Specificity} = \frac{TN}{TN+FP}. \tag{4}$$

Precision is calculated as the ratio of true positive data points to total points classified as change points,

$$\text{Precision} = \frac{TP}{TP+FP}. \tag{5}$$

The difference in time between estimated segments' boundaries and the actual change points can be treated as performance measure as well. In this case a number of useful metrics can be implemented. Mean absolute error (MAE) measures the distance of the predicted change point $\hat{y}_i$ to the actual change point y_i, i=1,…,N,

$$MAE = \frac{\sum_{i=1}^{N} |\hat{y}_i - y_i|}{N}. \tag{6}$$

Mean squared error (MSE) can take large values if a number of sufficient outliers occur in the classified data,

$$MSE = \frac{\sum_{i=1}^{N} (\hat{y}_i - y_i)^2}{N}. \tag{7}$$

Mean signed difference (MSD) evaluates the direction of the error, i.e. if the location of the predicted point before or after the actual time position of the change point,

$$MSD = \frac{\sum_{i=1}^{N} (\hat{y}_i - y_i)}{N}. \tag{8}$$

Root mean squared error (RMSE) accumulates square error between protected and actual change point and offset the scaling factor of squaring the differences,

$$RMSE = \sqrt{\frac{\sum_{i=1}^{N} (\hat{y}_i - y_i)^2}{N}}. \tag{9}$$

Two methods can be used to normalize root mean square error (NRMSE), namely using the range of the observed change points or the mean of observed change points,

$$NRMSE = \frac{RMSE}{max_i(\hat{y}_i) - min_i(\hat{y}_i)}, \tag{10}$$

$$NRMSE = \frac{RMSE}{\frac{1}{N}\sum_{i=1}^{N} \hat{y}_i}. \tag{11}$$

3. Main results

The data was examined in a tenfold stratified cross validation classification scheme, where 90 percent of the data was used to calculate features and train a naïve Bayes classifier which was then tested on the remaining 10% of examples. This procedure was repeated ten times and the overall result was calculated and is presented in confusion matrices in the following list.

As features for classifying we used: Mean, Variance, Kurtosis, Skewness, Interquartile range and autocorrelation from order 1 up to order 3. The performance measures (1)-(5) are denoted with an index, which represents the class such that the other two are merged to a single one. In this evaluation we assume that the time where the behaviour possibly changes and we only want to find the class of each segment

1. **Scenario 1:**

Table 1: Confusion Matrix for Scenario 1

Estimated Class **True Class**	**1**	**2**	**3**
1	**9838**	**155**	**7**
2	**207**	**9483**	**310**
3	**15**	**477**	**9508**

Table 2: Performance Measures for Scenario 1

Class	**1**	**2**	**3**
Accuracy	0.9872	0.9617	0.9730
Sensitivity	0.9838	0.9483	0.9508
Specificity	0.9889	0.9684	0.9841
G-Mean	0.9863	0.9582	0.9672
Precision	0.9779	0.9375	0.9677

2. **Scenario 2:**

Table 3: Confusion Matrix for Scenario 2

Estimated Class **True Class**	**1**	**2**	**3**
1	**7498**	**2337**	**165**
2	**2003**	**7667**	**330**
3	**15**	**186**	**9799**

Table 4: Performance Measures for Scenario 2

Class	**1**	**2**	**3**
Accuracy	0.8493	0.8381	0.9768
Sensitivity	0.7498	0.7667	0.9799
Specificity	0.8991	0.8739	0.9752
G-Mean	0.8177	0.8168	0.9776
Precision	0.7879	0.7524	0.9519

3. **Scenario 3:**

Table 5: Confusion Matrix for Scenario 3

Estimated Class **True Class**	**1**	**2**	**3**
1	**9905**	**42**	**53**
2	**2**	**9998**	**0**
3	**112**	**0**	**9888**

Table 6: Performance Measures for Scenario 3

Class	**1**	**2**	**3**
Accuracy	0.9930	0.9985	0.9945
Sensitivity	0.9905	0.9998	0.9888
Specificity	0.9943	0.9979	0.9973
G-Mean	0.9924	0.9988	0.9931
Precision	0.9886	0.9958	0.9947

4. **Scenario 4:**

Table 7: Confusion Matrix for Scenario 4

Estimated Class **True Class**	**1**	**2**	**3**
1	**9655**	**345**	**0**
2	**370**	**8249**	**1381**
3	**2**	**1474**	**8524**

Table 8: Performance Measures for Scenario 4

Class	**1**	**2**	**3**
Accuracy	0.9761	0.8810	0.9048
Sensitivity	0.9655	0.8249	0.8524
Specificity	0.9814	0.9091	0.9310
G-Mean	0.9734	0.8649	0.8899
Precision	0.9629	0.8193	0.8606

As we can see from Table 1-8, all 4 scenarios lead to good classification and high performance measures.

In addition to our fest set-ups, we also want to test for the quality of segmentation using our classification algorithm as described above. Therefore we defined a moving window of fixed length 100 and calculate for every time series in the testing set the classification result on series

$$(x_i, \cdots, x_{i+99}) \rightarrow c_i, i = 1,11, \cdots ,201,$$

which yields a sequence

$$(c_1, c_{11} \ \cdots, c_{201}), c_i \in \{1,2,3\}.$$

This sequence is transformed into a two class problem by either

$$2 \rightarrow 1 \ or \ 2 \rightarrow 3 \ .$$

Considering these sequences, we define change-points as points I s.t

$$c_i \neq c_{i+1}$$

and compare them with the actual change-point. We transform such points i to a change point j by

$$j = 10\ i + 45$$

and use j to calculate our performance measures (7)-(11), which can be found in Table 9:

Table 9: Change-point Performance Measures for Scenario 1-4

Scenario + Transformation	MAE	MSE	MSD	RMSE
1(2 → 3)	23.527	1025.5	2.3656	32.008
1(2 → 1)	29.865	1430.6	-14.417	37.823
2(2 → 3)	34.779	1856.8	13.764	43.091
2(2 → 1)	32.994	2116.7	-20.600	46.008
3(2 → 3)	22.860	815.01	-0.021398	28.549
3(2→1)	28.094	1211.5	-8.6860	34.807
3(2→3)	42.673	2664.7	38.41	51.621
3(2→1)	21.452	573.39	-20.484	23.946

4. Conclusion and Outlook

The classification results show quite good quality with high values for all considered performance measures, accuracy ranges from 83.81 % to 99.85 % in our experiments, while the sensitivity attains values from 74.98 % to 99.98 %. In all our scenarios the different states are thus rather easy to distinguish with only a small set of features.

Of course we have to tackle additional problems in case of real scenarios, like highly imbalanced data, more subtle changes and violation of model assumptions. Moreover our feature space is tailored to the changing properties of the time series, in real data the construction of appropriate features is crucial and a difficult task on its own. The change point performance measures are also satisfying, when we consider that if we chose change points random and uniformly on our possible *j*s, the resulting measures would be

MAE: 62.5 MSE: 5825 MSD: 50/-50 RMSE: 76.32

We expect that proposed methodology can be successfully implemented to real segmentation sensor measurements of different industrial machines used as technical elements of critical infrastructure to predict the anomalies and operational quality in realistic settings.

Acknowledgements

This work has been supported by the COMET-K2 Center of the Linz Center of Mechatronics (LCM) funded by the Austrian federal government and the federal state of Upper Austria.

References

[1] Abramson, M. (2015) Sequence classification with neural conditional random fields. IEEE 14th International Conference on Machine Learning and Applications (ICMLA), Miami, FL, pp. 799-804.

[2] Awad M., Khanna R. (2015) Support vector machines for classification. In: Efficient Learning Machines. Apress, Berkeley, CA.

[3] Bonaccorso, G. (2017) Machine learning algorithms. Packt Publishing.

[4] Brockwell, P.J. and Davis R.A. (1991) Time Series: Theory and Methods Springer Series in Statistics, pp.78-79

[5] Chandola, V., Banerjee, A. and Kumar, V. (2009) Anomaly detection: A survey. ACM Computing Surveys (CSUR) 41(3), 15.

[6] Engle, R.F. (1982) Autoregressive Conditional Heteroscedasticity with Estimates of the Variance of United Kingdom Inflation.
Econometrica 50 (4): pp. 987–1007.

[7] S. R. Gunn. (1997) Support Vector Machines for Classification and Regression. Technical Report, Image Speech and Intelligent Systems Research Group, University of Southampton.

[8] Keogh, E., Chu, S., Hart, D., Pazzani, M. (2004) Segmenting time series: A survey and novel approach. Data Mining in Time Series Databases 57, pp. 1-22.

[9] Khanteymoori A.R., Homayounpour M.M., Menhaj M.B. (2008) A Bayesian network based approach for data classification using structural learning. In: Sarbazi-Azad H., Parhami B., Miremadi SG., Hessabi S. (eds) Advances in Computer Science and Engineering. CSICC 2008. Communications in Computer and Information Science, vol 6. Springer, Berlin, Heidelberg.

[10] Mucherino A., Papajorgji P.J., Pardalos P.M. (2009) *k*-Nearest Neighbor Classification. In: Data Mining in Agriculture. Springer Optimization and Its Applications, vol 34. Springer, New York, NY

[11] Parsian, M. (2015) Data algorithms. O'Reilly Media Inc.

[12] Povinelli, R.J., Johnson, M.T., Lindgren, A.C. and Ye, J. (2004) Time series classification using Gaussian mixture models of reconstructed phase spaces. I In IEEE Transactions on Knowledge and Data Engineering, vol. 16, no. 6, pp. 779-783, June 2004.

[13] Sharma, H. and Kumar, S. (2016) A survey on decision tree algorithms of classification in data mining. International Journal of Science and Research (IJSR) 5(4).

[14] Wang, P., Wang, H., Wang, W. (2011) Finding semantics in time series. Proceedings of the 2011 international conference on Management of data - SIGMOD'11, June 12–16, 2011, Athens, Greece.

Index for asset value measure obtained from condition monitoring digitalized data interpretation. A railway asset management application

Pablo González
Department of Industrial Management, University of Seville, Spain
Camino de los Descubrimientos, s/n.
41092, Seville, Spain

Antonio Guillén
Department of Industrial Management, University of Seville, Spain
Camino de los Descubrimientos, s/n.
41092, Seville, Spain

Antonio de la Fuente
Department of Industrial Management, University of Seville, Spain
Camino de los Descubrimientos, s/n.
41092, Seville, Spain

Eduardo Candón.
Department of Industrial Management, University of Seville, Spain
Camino de los Descubrimientos, s/n.
41092, Seville, Spain

Pablo Martínez-Galán
Department of Industrial Management, University of Seville, Spain
Camino de los Descubrimientos, s/n.
41092, Seville, Spain

Adolfo Crespo.
Department of Industrial Management, University of Seville, Spain
Camino de los Descubrimientos, s/n.
41092, Seville, Spain

Abstract

The objective of any asset is to provide value to the organization, being the corner stone to get a highest possible economic benefit in a sustainable way. An effective asset value management demands method that allow measuring and comparing the expected value with the real value realized at any time during its life cycle for value informed decision-making. Digitalization is providing new data about events and states related to asset condition and risk, information that can be reinterpreted to generate value measure strategies. This paper presents a proposal of TVO (Total Value of Ownership) model where it is possible to quantify and measure the value, including its monitoring throughout the life cycle of the asset and/or system.

Proposed TVO model is focused on Safety, one of the most relevant value factors for Industry and Infrastructure sectors. Asset events and states are intrinsically linked to the defined failure modes. Consequently, it is necessary to structure the system information around the failure modes that have been defined, in order to obtain a value measurement index. A railway use case is presented.

Keywords: TVO, Condition Monitoring, Value Based management

1. Introduction

The aim of this paper is to present a case of a quantitative asset management tool consisting of obtaining a value measurement index. The index proposal and its use are linked to the use of TVO models to support decision making in the central phase of the life cycle of an asset or MoL (Middle of Life) (Roda et al., 2015). These models are connected to the best known TCO models. TVO proposes and emphasizes management by value, in accordance with the postulates of the ISO 55000 standard, as opposed to an exclusive management based on the economic costs of the TCO. The application of TCO in the industry and other sectors is mature while the TVO models are much scarcer and there is not enough consensus either on their design, calculation or their application in decision making (Srinivasan and Parlikad, 2017). This paper tries to make a contribution in this sense.

At the same time, digitization makes new capabilities available to organizations. It highlights, in a significant way, the possibility of developing new models of data and information not available until now. In particular, this digitization allows the development of new uses of data extracted from a monitoring system. This study proposes the connection of monitoring with the calculation of an index to measure the value that is reliable to the organization, on which to make decisions and control the outcome of them in the medium and long term.

The paper is structured as follows: the following section briefly reviews the key aspects and concepts about the developments of this work. Section 3 presents the methodology used to obtain the value index related to safety; Section 4 briefly presents a practical case that has served as support for the development of the model. Finally, Section 5 includes the main conclusions of this work.

2. Background

"Value" is one of the key concepts in asset management (Roda et al., 2015). The international standard ISO 55000 (ISO, 2015) establishes that asset management promotes the contribution of value, and defines the asset as the element that has or generates value for the organization. Asset management should be conducted around value control. To this end, each asset has to be managed and defined according to the concept of the organisation’s own value that it itself establishes (Sola et al. 2015). The definition of the value of each organization makes it possible to define which are those assets and in what way they contribute to obtaining the expected value or its conservation (IAM 2010). However, there are currently not many management tools that integrate the concept of value, and in most cases economic indicators are used as the basis for decision-making. Therefore, it is necessary to deepen in the development of new indicators and methodologies that allow the objective measurement of value in order to be able to manage the assets around this concept in an efficient and effective way (Gonzalez-Prida et al., 2019).

The Total Cost of Ownership (TCO) is the sum of all costs incurred by the owner of a physical asset throughout its entire life cycle (Ellram, 1995). These costs are those required to acquire, install, commission, operate, maintain and finally dismantle the equipment (Duran et al., 2016). All these costs play an important role in the decision-making process, especially in aspects such as maintenance planning, spare parts purchasing and operating strategies among others. In addition, it has been proven that the TCO can serve as a support tool for management, obtaining a measurement and reduction of costs (Bacchetti et al., 2018). The TCO is a cumulative cost index as it includes all the costs associated with the life cycle of an asset. It makes it possible to estimate and monitor the cost in its different phases.

The Total Value of Ownership concept extends the TCO approach to the monitoring and control of aspects of value such as social and environmental impact, as well as the economic aspect as offered by the TCO (Srinivasan and Parlikad, 2016). While the TCO only provides information for economic management while the TVO allows a management focused on the value that is promulgated by asset management (ISO, 2015). The management focused on the TVO allows maximizing the operation for a certain budget, while the management focused on the TCO, minimizes the budget to maintain a certain level of operation (Srinivasan and Parlikad, 2017). As a result, the TCO makes it possible to maintain a level of service while the TVO tries to obtain the optimum level of service. The difficulty of implementing a management system based on value versus cost lies in the concepts used, the second are consolidated in the industry while the first are not.

The processing of events/states is the basis for the quantitative indicators that maintenance engineering uses. In fact, the RAMS (Reliability, Availability, Maintainability and Safety) analysis methodology is based on the management of a set of indicators obtained from the evaluation of the characteristic times of the operating and fault states that, in turn, limit the events of failure and repair (Parra and Crespo, 2012). A failure occurs when an asset fails to perform its required function (Birolini, 2017). On the other hand, the term to define the state of inactivity is not the failure, it is the fault (Figure 1). As schematized in Figure 1, repair is an event that returns the asset to the operating state. This same event/state scheme can be used in a more general way to model intermediate states generated from available information through monitoring techniques that give access to detailed knowledge about the asset degradation process until failure.

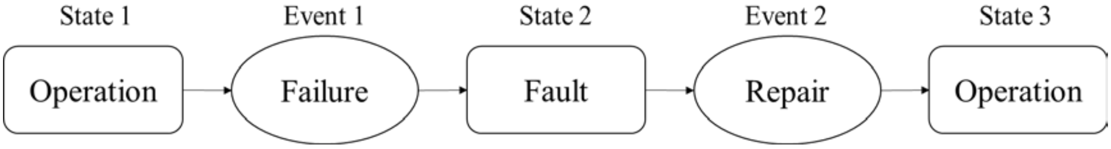


Figure 1. Basic states and events of RAMS analysis methodology.

Condition-based maintenance (CBM) is a monitoring-based maintenance strategy that focuses much of the digitization efforts of maintenance, especially in the development of predictive solutions or PHM (Prognosis and Health Management) (Jardine et al., 2006). Technological development has made it possible to reduce the costs of sensors and systems that measure assets, making it possible to obtain data on assets considered critical. The monitoring and analytical techniques used in the CBM make it possible to control the risk of failure and predict the time to failure or RUL (Remaining Useful Life) (Guillen et al., 2016). Risk is the product of the probability of occurrence of a failure and its consequence (Crespo, 2007). Condition monitoring is linked and allows to control the probability factor. A specific monitoring measure may indicate a higher probability of failure and, therefore, a higher risk. It is the identification of different levels of risk that supports maintenance decision making. These levels are defined from reference values or thresholds.

Similar to what happens with failures and times between failures in the RAMS methodology, the new events and states identified through monitoring and their thresholds allow handling events and intermediate states between operation and fault states. The management of these states and their characteristic times can give rise to new indicators of interest for management. These include objective quantitative measures of value. In this way it is possible to link condition monitoring to value-based decision making.

3. Methodology for the calculation of the TVO

This methodology connects the result of the monitoring to the evaluation of the TVO. It can be understood as part of an information management strategy aimed at generating new information for the digitization of decision-making processes.

It is necessary to establish a structure of information related to the asset in order to make full use of all available data provided by monitoring. Three pillars or fundamentals of description have been taken into account in the modelling of asset-related information:

- Objective definition of value. Generation of value measurement index.
- Failure mode as object of maintenance. Any data is interpreted in relation to the failure mode or the failure modes it affects.
- Events and states of failure modes. The value index measurement itself refers to the failure mode. Events and states appear as a result of monitoring and their interpretation at risk levels for each failure mode. The interpretation of the risk levels translates into a measure of the value index.

The methodology includes the following steps illustrated in Figure 2:

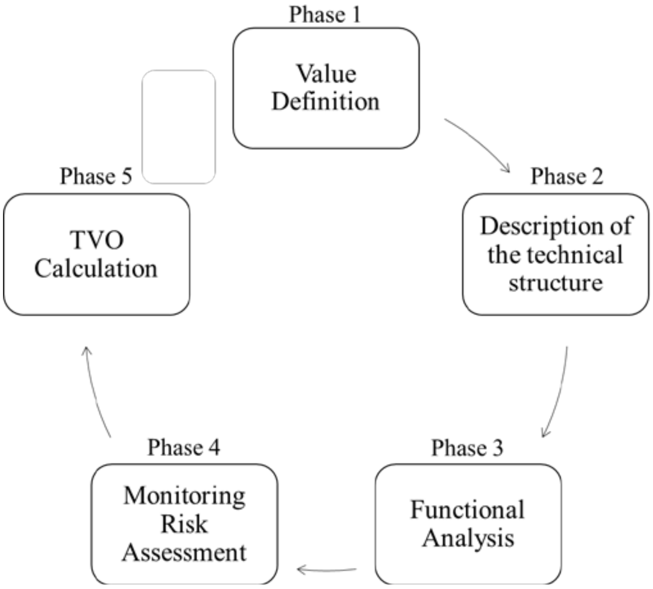


Figure 2. Steps of the proposed methodology.

Phase 1. Value Definition. First of all, it is necessary to define the concept of value according to the objectives and principles of the organization. The organization provides the most important factors related to its activity (e.g. safety, environmental impact, quality of service, etc.). These factors will allow to define the value for that organization, being different in each organization. Each factor can be parameterized in a series of measurable indicators in all assets. The evaluation of the criticality of the assets will be carried out from the defined factors. The definition of the factors has a double functionality: (i) the evaluation of the criticality and hierarchization of assets by value; (ii) the calculation of the TVO. In the practical case, a value measurement index will be generated around the Safety factor, as will be seen later.

Phase 2. Description of the technical structure. The system is broken down into the different levels of intervention that make up its technical structure. The intervention levels try to describe in a precise way the element to maintain within the technical structure. These levels will then make it possible to determine at what level certain maintenance policies are applied. The correct definition of the intervention level conditions all subsequent decisions (López, 2018).

Phase 3. Functional Analysis. It allows to obtain a description of failure modes linked to the general system through the technical structure. The failure mode is the basic element in maintenance management. Each unit performs one or more functions. The failure mode is associated with a maintainable component of an equipment. For each function performed by an equipment, there are as many failure modes as there are maintainable components in the equipment (López 2018).

Phase 4. Monitoring Risk Assessment. The methodology proposes the interpretation of monitoring, generating risk indicators and rules of interpretation on these indicators. It is possible to define different levels of risk through thresholds or reference values, introducing new intermediate states between operation and fault. A risk level is therefore the representation of a state. This begins with the event that a threshold is exceeded and ends when the indicator leaves that level. This level change may be due to a new higher risk threshold being exceeded (progress in degradation) or due to a reduction in the risk level (reduction may be due to maintenance action or spontaneous favourable evolution) (Figure 3). Figure 3 shows that when a critical risk level is reached (corresponds to a critical value), maintenance is carried out to avoid failure and ensure operation.

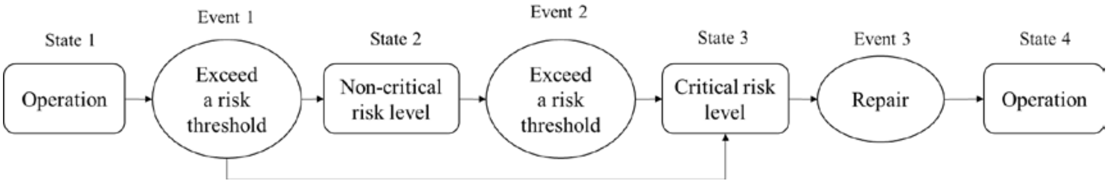


Figure 3. States and events according to methodology.

Phase 5. TVO Calculation. In order to carry out a measurement and a control of the value, the TVO concept will be used. This concept allows to relate the measurement of the value with the life cycle of the asset being of great help for decision making in the medium and long term.

The proposed TVO model focuses on giving a measure of the value factor "Safety", although it would be possible to develop similar indices for any other value factor. The ISG is defined as a quantitative index that measures the total of equivalent days in which an asset or group of assets is at its maximum level of safety considering:

- The maximum safety in an asset (100 % or 1) corresponds, at all times, to the theoretical maximum safety, i.e. the state in which the asset does not present any objective circumstance involving a risk of a significant reduction in safety.
- Each level of risk determined as a result of monitoring is assigned a specific percentage decrease in safety. This interpretation is carried out with the participation of expert personnel in the installation. In this way, depending on the level of risk at which an asset is located, it is possible to know how much safety has been reduced.
- Equivalent days: the safety reduction is computed in days, so that, if during a calendar day of an asset has been at 50% of its maximum safety level, only 0.5 days will be added to the ISG calculation.

The model used for calculating the indicator is shown in the following statement:

$$\sum_i ISG_i\,(\Delta t) = \sum_i \big(DT_i(\Delta t) - \sum_j DSD_{ij}\big) \qquad (1)$$

$$DSD_{ij} = DD_{ij} * Cc_i * Css_j \tag{2}$$

Where:

- i: asset on which the safety fault is identified.
- j: failure mode detected.
- DT_i: total days in the period considered.
- DD_{ij}: estimated days from the beginning of the problem.
- DSD_{ij}: equivalent days of reduced safety.
- Css_j: Severity of the failure by Safety 0-1.
- Cc_i: Criticality coefficient of asset i, 0-1.

As it was being searched for, it is a value measurer. It is related to the value factor Safety, defined during the design of the corresponding asset management model. It is a cumulative index, similar in this sense to the cost that serves as the basis for the TCO models. In this way it is possible to treat the accumulated ISG throughout the life cycle or the ISG during a certain period of time or until a certain date.

4. Use case

In the practical case, the proposed methodology is applied in the railway field, in particular on metro lines. For this purpose, information on a metro line is available. Information is available on the technical structure and parameters associated with the equipment contained therein. On the other hand, information is available on the set of factors in which the organisation has broken down its concept of value, which will allow the criticality of the functional locations to be evaluated.

Between value factors, safety is the most important factor. This makes it possible to focus the study on the measurement of safety, leading to the creation of a total value model based on this factor. This need to generate the model around safety is justified in the following statements:

- In railway systems in general, and in the metro in particular, safety is paramount.
- If safety is diminished or reduced, it does not necessarily mean that a failure or accident occurs.
- On the other hand, what it does imply is that during the safety degraded state, safety is not satisfied to its maximum possible level.
- It has been observed that the non-detection of failures or their non-appearance hide reductions in safety. This mask the results of the evaluation of asset performance and maintenance. In this way, circumstances that may be important for the effective control of risk and safety are not taken into account in decision-making or in proposals for improvement.

In order to carry out the practical case, a system has been generated that allows the management of assets. This system allows the processing of the information transmitted by the on-board monitoring system. Before receiving and processing the information transmitted by the monitoring system, it is necessary to define the first three phases proposed in the methodology. This allows the system to have the necessary premises to carry out the remaining phases.

Phase 1. For the railway case under analysis, a set of value factors has been defined. The factors defined are: safety, social and environmental impact, integrity and life cycle, operation and quality of service and cost of corrective maintenance. Each factor, according to the organisation's criteria, has been assigned a percentage, the sum of these percentages being 100%. The organisation has defined that 40% of safety has been assigned, the main reason for which a safety-centred value measurement index has been developed.

Phase 2. In order to define the technical structure, it was necessary to define the levels of intervention. The intervention level is the one at which the maintenance policies will be applied. At the same time, this precisely determines the object of the analysis. The existing model of the railway track did not provide enough information, and it was necessary to obtain a new model. A total of seven levels of intervention have been defined: line, section, subsection, system, subsystem, equipment and component. In this way, the elements where the maintenance activities are carried out are precisely defined. The sub-section level allows to distinguish curves and slopes with specific operating conditions and degradation modes that can be related to monitoring.

Phase 3. For each of the assets that compose the system, a study has been carried out on the different failure modes that can take place in them. Some of the failure modes that occur on a railway track are illustrated below: cracked track, worn track or dirty track. These failure modes have been defined on the basis of the history of failure modes and the advice of technical experts in railways.

Phase 4. In order to evaluate the risk of failure due to a failure mode in an asset three requirements are necessary: (i) define a set of risk indicators whose thresholds are defined by the value of the monitored parameters (e.g. length of serious defect if the value is greater than 40 mm); (ii) an on-board monitoring system that transmits the information in real time; (iii) use logical rules of interpretation (combination of AND or OR types) of the defined risk indicators to assess the risk in each failure mode (e.g. the risk level is high for the failure mode "Cracked track" if the risk level of the "defect length" indicator is high and the risk level of the "defect width" indicator is medium).

The graph to the left of Figure 4 shows the time evolution of a risk indicator. The colours grey, green, yellow and red are associated with zero, acceptable, medium and high risk levels respectively. It can be observed how for this risk indicator, along the analysed temporal horizon, its risk level increases until a maintenance action is carried out reducing the risk to 0. The graph to the right of Figure 4 shows the duration of each risk level of each failure mode for all assets analysed. The graph shows the duration of the risk levels for the "Dirty track" failure mode of the different assets.

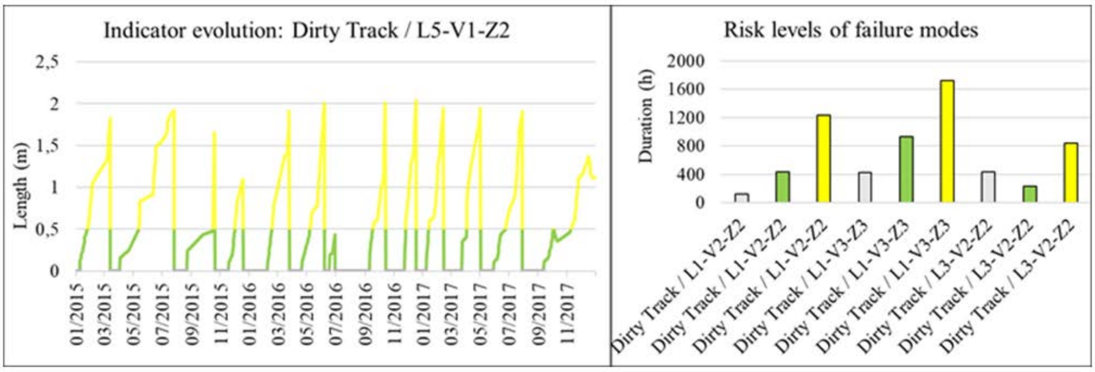


Figure 4. On the left, representation of the evolution of a risk indicator in the analysed time horizon. On the right, the duration of the risk levels of a multi asset failure mode.

Phase 5. The duration of the different levels of risk has a translation that is reflected in the measure of the value index, in this case, of the ISG. Thanks to the on-board monitoring system, a real-time measurement of the value can be obtained. The system is able to draw a graph where the comparison of the real value in real time and the theoretical value of the ISG is carried out. Also, it shows the value of the real TCO against the theoretical one in real time (Figure 5).

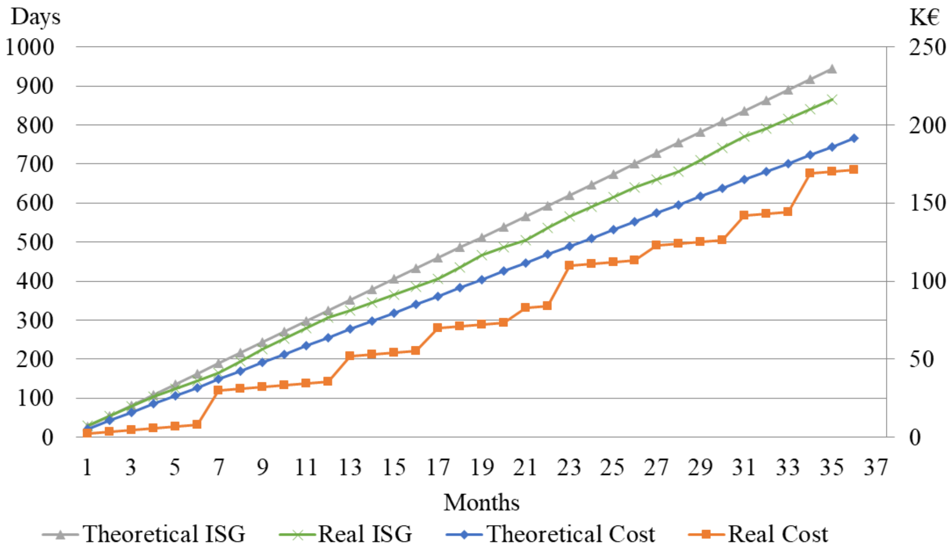


Figure 5. Theoretical and actual ISG and TCO on the analysed time horizon (ISG referred to left axe and TCO referred to right axe).

The decision-making process for carrying out maintenance activities will be conditioned by two interrelated measures: the level of risk of an asset and the value of the asset's ISG.

5. Conclusions

Value is a concept inherent to each organization that depends on its objectives, being difficult to quantify because there is no general procedure for defining it. On the other hand, existing asset management tools and models allow decisions to be made based exclusively on economic value, not on the value of the organization. In order to define value in a clear and concise way, an asset management tool is proposed where information is structured around failure modes and events that take place in the assets. Consequently, an intelligent asset management system has been developed with the mentioned approach, being used in a practical case in the railway field.

Monitoring makes it possible to know the state of the assets and, consequently, to know the level of risk they have at any given moment. The duration of the different risk levels of the assets has a translation in terms of equivalents days of security. The value of the ISG is proportional to the equivalent days of safety. The measure of the value in terms of security can be done through the ISG. By comparing this value measurement with the theoretical value calculated at the beginning of the life cycle of the asset, the operation of the asset can be evaluated and, where appropriate, acted upon. In this way it is possible to link condition monitoring to value-based decision making.

References

Bacchetti, A., Bonetti, S., Perona, M., Saccani, N. (2018) *Investment and Management Decisions in Aluminium Melting: A Total Cost of Ownership Model and Practical Applications*. Sustainability 2018, 10, 3342.

Birolini A. (2017) Basic Concepts, Quality & Reliability (RAMS) Assurance of Complex Equipment & Systems. In: *Reliability Engineering*. Springer, Berlin, Heidelberg

Crespo, A. (2007) *The Maintenance Management Framework Models and Methods for Complex Systems Maintenance*. London: Springer London. pp. 111-112. https://doi.org/10.1007/978-1-84628-821-0

Duran, O., Roda, I., & Macchi, M. (2016). *Linking the spare parts management with the total costs of ownership: An agenda for future research.* Journal of Industrial Engineering and Management, 9(5), 991-1002.

Ellram L., (1995) *Total cost of ownership: an analysis approach for purchasing.* International Journal of Physical, Distribution & Logistics Management, Vol. 25 Issue: 8, pp.4-23, https://doi.org/10.1108/09600039510099928

González-Prida, V., Guillén, A., Gómez, J., Crespo, A., & de la Fuente, A. (2019). *An Approach to Quantify Value Provided by an Engineered Asset According to the ISO 5500x Series of Standards*. In Asset Intelligence through Integration and Interoperability and Contemporary Vibration Engineering Technologies (pp. 189-196). Springer, Cham.

Guillén, A. J., Crespo, A., Gómez, J. F., & Sanz, M. D. (2016). *A framework for effective management of condition based maintenance programs in the context* *of industrial development of E-Maintenance strategies*. Computers in Industry, 82, 170-185.

IAM (2011). *Asset Management - An Anatomy,* Institute of Asset Management, UK

ISO (2015). ISO 55000:2015a. *Asset management - Overview, principles and terminology*.

Jardine, A. K., Lin, D., & Banjevic, D. (2006). *A review on machinery diagnostics and prognostics implementing condition-based maintenance*. Mechanical systems and signal processing, 20(7), 1483-1510.

López, A. J. G. (2018). *Diseño de soluciones avanzadas de CBM/PHM en sistemas inteligentes de gestión de activos* (Doctoral dissertation, Universidad de Sevilla), pp 66-79.

Parra, C., & Crespo, A. (2012). *Ingeniería de Mantenimiento y Fiabilidad aplicada a la Gestión de Activos*. INGECON

Roda I., Parlikad A., Macchi M., Garetti M. (2015). *A Framework for implementing value-based approach in Asset Management,* Proceedings of the 10th World Congress on Engineering Asset Management (WCEAM 2015). Part of the series Lecture Notes in Mechanical Engineering pp 487-495.

Sola, A., Crespo, A., Guillen, A. (2015) *Bases para la mejora de la gestión de activos en las organizaciones*. Industria Química.

Srinivasan, R., Parlikad, A.K. (2016).*Whole-life Value-based Decision making in Asset Management*, ICE Publishing, ISBN: 9780727760616, 96 pages.

Srinivasan, R., Parlikad, A.K. (2017). *An approach to value-based infrastructure asset management*, Infrastructure Asset Management, Volume 4, Issue 3, pp 87-95.

Advances in vulnerability assessment of coupled gas and electricity transmission networks by using graph theory

Jose M. Yusta[1], Jesus Beyza[1,2], Jose A. Dominguez-Navarro[1], Rodolfo Dufo[1], Jose L. Bernal-Agustin[1]
[1]University of Zaragoza, Dept. of Electrical Engineering
C/ Maria de Luna 3
E-50018, Zaragoza, Spain
[2]Morelia Institute of Technology, Dept. of Electrical Engineering
Avda. Tecnologico 1500
E-58120, Morelia, Mexico

Abstract

The main purpose of the REDCRIT research project (http://redcrit.unizar.es/) is the development and validation of a vulnerability assessment methodology for the topology of interdependent energy infrastructures against random faults and intentional attacks. For this purpose, the use of graph theory is proposed by calculating the geodesic vulnerability indicator in the topology resulting from the simulation of successive cascading failure contingencies in a coupled infrastructure of gas and electricity networks in Spain. The methodology developed has been applied to real gas and electricity transmission networks in Spain, and the coupled network results more vulnerable than the electrical network. In addition, the vulnerability of the new topologies resulting from the construction of new power lines and gas pipelines up to 2020 has been evaluated.

Keywords: graph theory; cascading failures; critical infrastructure

1. Introduction

Infrastructure does not exist in isolation; these structures are interconnected with each other. Technological advances make infrastructure components increasingly complex and mutually dependent. Once a system suffers a fault, either by external or internal disturbances, the fault can spread very quickly to other systems. Therefore, the increased interconnection between critical infrastructure systems has made them more vulnerable.

In 2008, the European Directive 2008/114/EC “on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection” [1] warned about the possible impact of the effects resulting from the interdependency between interconnected infrastructures.

Among the infrastructure systems under analysis and protection, energy networks play a major role, since energy is the economic engine that sustains modern society. To protect critical energy infrastructure, comprehensive risk management programmes must be developed, beginning with vulnerability analysis and risk assessment, both for system faults and intentional threats.

The risk assessment stage should be as objective as possible, which requires quantitative tools that allow assessing risks expected to affect network operations, including both possible power outages due to severe weather conditions and technical faults such as intentional attacks on infrastructure. These risks can cause problems in one or more infrastructure components, so it is necessary to estimate the weakness of the system with respect to a cascading sequence of events to analyse the vulnerability of the energy system [2].

A more realistic simulation model provides a closer representation of the system under study and a better representation of the system under extreme conditions. However, greater realism also implies greater complexity in the models [3]. Alternatively, a more abstract model, although simpler, provides the foundations for more detailed models. In that sense, the models built on graph theory provide a new perspective regarding critical infrastructure systems.

Many critical infrastructure systems can be represented by a network of interconnected nodes through links. Graph theory or complex networks [4,5] in electrical networks facilitate the analysis and visualisation of physical behaviour, for instance, the assessment of cascading failures by studying the topology of the system and the evaluation of impacts due to the removal of specific components in a system and their consequences in power-flow congestion.

Important research efforts in recent years have focused on the modelling of energy systems as complex networks. The definition of scale-free networks, initially proposed in [4], was followed by the application of new concepts of statistical measures, vulnerability analysis and resilience estimation, with applications in different engineering problems [5,6,7]. In [8], the cascading failure problem in scale-free networks was formulated by modelling a node removal strategy in a network following the nodal degree, which was the basis for developing the vulnerability assessments of electrical power networks [9].

However, [10,11] demonstrated that the statistical measures of graph theory (clustering, connection degree, geodesic distance, and nodal distribution) are adequate for the vulnerability assessment of an energy system and particularly for cascading failure analysis.

Other researchers have used alternative measures for complex network models; for instance, in [12], the use of geodesic efficiency indicators is suggested for the analysis of cascading failures. Another approach suggested is to measure the betweenness of the graph [13].

Among the electrical network models based on graphs, certain studies have been carried out in Nordic countries [10,14] and on the electrical network of continental Europe [15] where the advantages of using topological indicators (clustering, geodesic distance, and geodesic efficiency) to analyse the vulnerability of an electrical network are demonstrated.

Therefore, modelling with complex networks has become an accepted methodology for conducting protection studies on energy networks facing certain threats [16,17].

In recent years, certain research studies have been focused specifically on modelling interdependent infrastructure systems. In the scientific literature, there are several concepts of interdependency between infrastructure systems based on the existence of physical, logical, bidirectional, and unidirectional dependency [18-20]. However, the analysis and simulation of the planning and combined operation of electric power and gas transmission systems have also been the subject of attention in recent years [21-23].

2. Research proposal

Complex network theory has proven to be useful for the study of topology characteristics of different interdependent infrastructure systems [24] and in particular can be useful for vulnerability analyses of power supply networks [25]. However, this research field is so new that there are only a few specific methodologies and applications regarding combined gas and electricity transmission networks from the point of view of robustness and resilience. Currently, these networks are highly interconnected by electricity generation expansion in combined-cycle natural gas power stations, which makes them strongly interdependent. In Spain, 25% of the installed electric power from generation stations corresponds to natural gas power stations. In addition, these networks are part of the critical infrastructure, whose disruption would have direct impacts on the economy, and due to the nature of the interdependency, a cascading failure in one network can quickly and catastrophically spread to the others.

The main objective of the REDCRIT project (http://redcrit.unizar.es/) is the development and validation of a vulnerability assessment methodology for interdependent energy infrastructure topologies and the application of this methodology to the improvement of the resilience of coupled electricity and natural gas transmission systems, using the previous results from the research group to replace the power-flow computational tools traditionally used for the analysis of contingencies in electrical networks with new methods based on complex network theory. This approach allows a rapid evaluation of network disintegration in the event of N-*k* contingencies, that is, in cascading failures of networks.

Vulnerability is a concept widely studied in many research areas. In this study, vulnerability is defined as the general susceptibility of a system to a specific event, that is, the magnitude of the consequences given the incidence of that event. Vulnerability must be related to a certain event to be meaningful. A system could be vulnerable to certain faults but could be robust and resistant to others. That is why this project proposes to estimate the vulnerability using simulations of random faults and intentional attacks on different elements of the infrastructure.

3. Methodology of the structural vulnerability analysis

The behaviour study of a scale-free network before an event is based on the disintegration analysis, calculating certain statistical indicators in the process of systematic removal of nodes by successive iterations, either randomly or deliberately. Each removal is associated with a contingency and is considered to be an iteration in the network disintegration process. The removal of a node also implies the disappearance of all the links that connect to that node; therefore, the respective geodesic paths also disappear.

In this project, different statistical measures that describe scale-free graphs that allow for network disintegration evaluation have been analysed, that is, their evolution before the successive removal of nodes. The robustness of a network is generally measured according to the size of the largest connected network before and after a cascading failure [6]. The analysis of these contingencies requires the use of the statistical parameters of graphs that allow for measuring the functionality of the networks.

In this project, the geodesic vulnerability index ($\bar{v}$) has been chosen to measure the functionality of the coupled electricity and gas network when the network is subject to a contingency. These indexes have been validated in previous studies on IEEE test networks [26] and subsequently applied to real electrical networks [27] by the same research group. However, these indexes have not yet been applied to coupled networks.

The geodesic vulnerability ($\bar{v}$) allows for the normalisation of the geodesic efficiency and balancing in the evolution process of node removal, as indicated in (1):

$$\bar{v} = 1 - \frac{\sum_{i \neq j} \left(\frac{1}{d_{ij}^{LC}} \right)}{\sum_{i \neq j} \left(\frac{1}{d_{ij}^{BC}} \right)} \tag{1}$$

where d_{ij}^{LC} is the geodesic distance between the node pairs of the scale-free graph after each iteration of node removal, and d_{ij}^{BC} is the geodesic distance between the node pairs of the scale-free graph for the base case.

The geodesic distance is described as the shortest direct path between two nodes by counting the minimum number of nodes that must be covered to join the two nodes. The index ($\bar{v}$) varies between zero and one. The higher this index, the greater the impact on the power supply interruption in the coupled network.

The performance of the coupled electricity and gas network, quantified by the geodesic vulnerability index in (1), is determined as a function of the fraction of nodes removed (*f*).

4. Application in the Spanish electricity and natural gas transmission networks

The structural vulnerability measure was applied to the interconnected electricity and natural gas transmission networks in Spain, subjecting the topology of the networks to cascading failures and analysing the robustness of the respective network expansion plans. Therefore, the network disintegration experiments were carried out only under the perspective of complex network theory.

This application incorporates all the assets and nodes of a single graph (power stations, substations, transmission towers, transformers, regasification plants, compression stations, gas pipelines, and consumption points) without considering physical distances or technical parameters (impedances, flows, or pressures).

4.1. Representation of the 400-kV electrical network

To represent the electrical network in Spain, the data provided by the system operator were considered [28]. Fig. 1 a) shows the proposed representation of the 400-kV electrical infrastructure in Spain. The graph is composed of a total of 611 nodes and 672 links. This representation considers not only the buses as assets but also the power lines, transformers, loads, and generators. The network created in this way allows for a detailed vulnerability analysis. In addition, all the assets of the electrical network may be candidates for attack.

4.2. Representation of the 80-bar natural gas network

The topology of the high-pressure natural gas network was obtained from [29]. To adequately represent this system, 6 regasification plants, 19 compression stations, 3 underground storage facilities, 2 reservoirs, 6 international connections, 32 direct-line connection points, 57 transmission-transmission connection points and 294 transmission-distribution connection points were considered. Fig. 1 b) shows the proposed representation of the high-pressure natural gas infrastructure in Spain. The proposed graph is composed of 1380 nodes and 1402 links. The network created considers all the main assets of the natural gas infrastructure.

4.3. Representation of coupled infrastructure

Fig. 1 c) represents the coupled electricity and natural gas network in Spain. The final graph is composed of 2031 nodes and 2154 links. Combined-cycle power stations of natural gas and electric compressors act as couplings for the described networks:

- In Spain, 25% of the installed electric power comprises gas power stations. The infrastructure includes a large number of this type of installation connected to substations with different voltage levels. In this study, only the 26 combined-cycle power stations that distribute their production to the 400-kV network were considered.
- However, the natural gas infrastructure includes 14 compressors that operate using electric power connected to the nearest electrical substations.

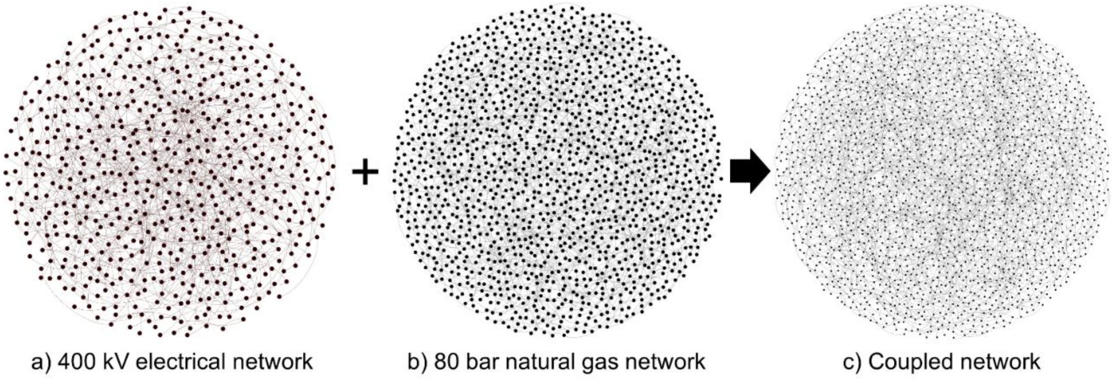


Figure 1. Graphs of electricity and natural gas transmission networks in Spain (taken from [31]).

4.4. Results

The structural vulnerability of the electricity and natural gas network in Spain was evaluated, considering the separate systems and the coupled system. Thus, the following cases arise:

- Simulation of the cascading failures in each separate electricity and natural gas network (cases 1 and 2).
- Simulation of the cascading failures in the coupled electricity and natural gas network (cases 3 and 4).

The interdependent effects were not considered in the simulation of cascading failures in the separate networks (cases 1 and 2); however, these effects were considered for the coupled network (cases 3 and 4). The results are presented both for intentional attacks on the networks and for random faults.

Fig. 2 shows the simulation results of cascading failures for the electrical (case 1) and natural gas (case 2) networks and for the combined coupled network (case 3). Figs. 2 a), c) and e) include the results for random faults, while Figs. 2 b), d) and f) correspond to the deliberate faults. Random errors correspond to random phenomena, such as human errors, adverse weather conditions, and equipment faults. On the other hand, intentional attacks include acts of terrorism, cyber-attacks, and malicious acts.

To comply with the central limit theorem requirement that guarantees an appropriate statistical sample, the results were obtained by averaging a set of 100 tests in case of random errors. However, intentional attacks only require removing the most strongly connected nodes in descending order of nodal degree.

The graphs in Fig. 2 represent the geodesic vulnerability value ($\bar{v}$) as a function of the fraction of nodes removed *(f)*. When all the nodes of the network are initially connected, the geodesic vulnerability ($\bar{v}$) is 0. As the network decomposes, because of the cascading disintegration, the value of the geodesic vulnerability ($\bar{v}$) increases to 1 when the power supply to all the nodes of the system has been interrupted.

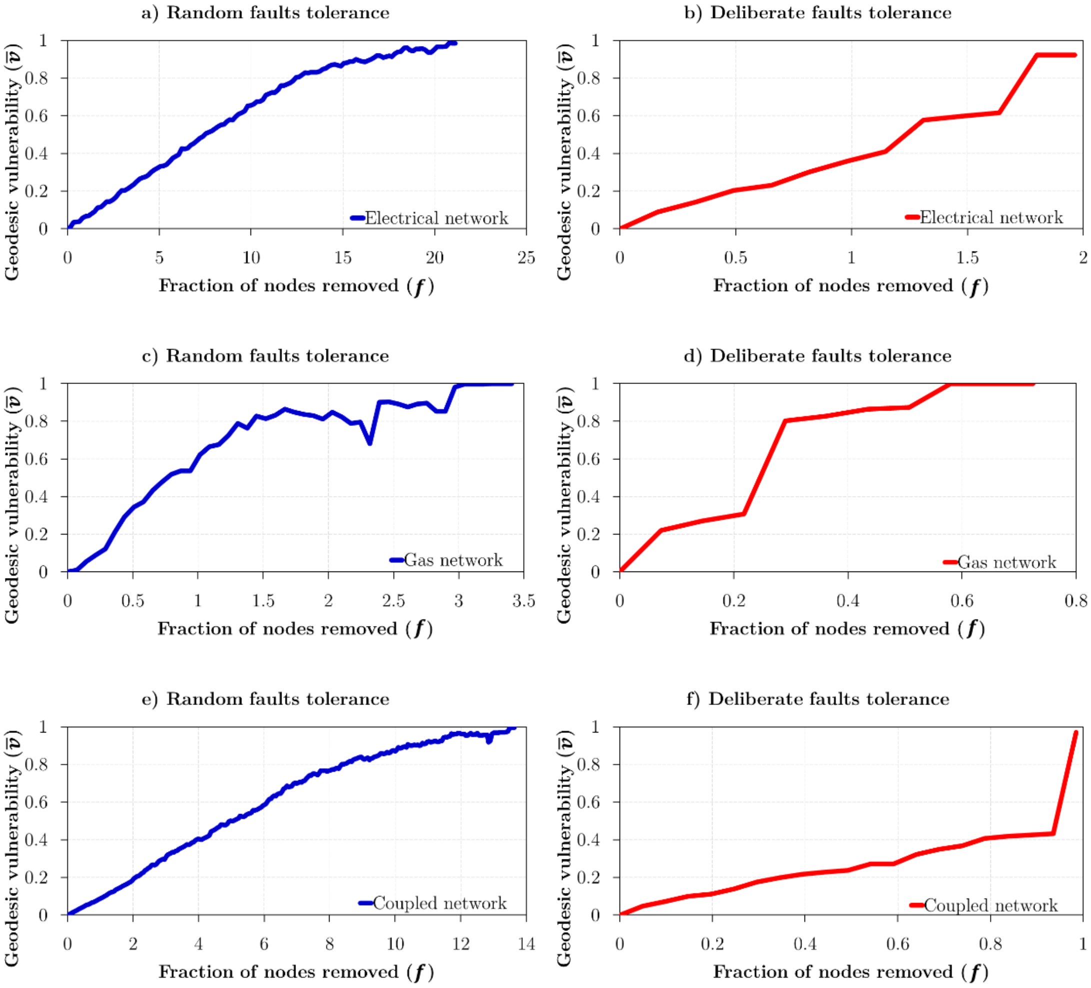


Figure 2. Simulation results for cascading failures in real gas and electricity networks in Spain.

Fig. 2 a) shows that the electrical network collapses to random faults with the removal of approximately 20% of the nodes. In the same electrical network, for deliberate faults, Fig. 2 b) shows that the removal of less than 2% of the nodes is sufficient for the network to collapse. The previous analysis shows that targeted attacks on high connectivity nodes are an effective tactic to rapidly disintegrate the networks.

However, Fig. 2 c) shows that the natural gas network collapses completely in the event of random faults when approximately 3% of the nodes in the network are removed. The results show that this system is more vulnerable than the electrical network. Meanwhile, in the face of deliberate faults, the removal of 0.7% of the nodes causes the disintegration of the network, as shown in Fig. 2 d). In these simulation cases, the natural gas network is less robust than the electrical network, which is explained by the different structures of the networks; the natural gas system has a smaller meshed topology than the electrical system.

Analysing the two networks in a coupled way (case 3), Fig. 2 e) shows that the network collapses to random faults with the removal of approximately 14% of the nodes in the network. However, Fig. 2 f) shows that the removal of 1% of the nodes is sufficient to completely collapse the network for deliberate faults.

5. Evaluation of the expansion plans for the Spanish electricity and natural gas transmission networks

In the REDCRIT project, the vulnerability of the coupled infrastructure of the gas and electricity transmission networks in Spain was also evaluated, considering the expansion plans proposed by network operators to improve the power supply security. The geodesic vulnerability measure was applied to the interconnected systems of electric power and natural gas, calculating the $(\bar{v})$ indicator in random cascading failures for each new topology resulting from the investment plans of the networks for the years 2018-2020 [30].

In this evaluation, 22 case studies were considered, corresponding to the construction of new 400-kV high-voltage power lines and 80-bar high-pressure gas pipelines between 2018 and 2020. Table I shows the results for different case studies corresponding to the removal of a certain number of nodes in the network (*f)*, the impact on the disconnection of the loads from the system by means of the geodesic vulnerability index $(\bar{v})$, and the f_{max} value, where the final disintegration of the system occurs [31].

Table I: Simulation results for random errors based on the fraction of nodes removed (EL: new power line, GL: new pipeline)

Case	**Asset**	$\langle \boldsymbol{f} = \mathbf{2}\% \rangle$	$\langle \boldsymbol{f} = \mathbf{4}\% \rangle$	$\langle \boldsymbol{f} = \ \% \rangle$	$\langle \boldsymbol{f} = \mathbf{8}\% \rangle$	$\langle \boldsymbol{f} = \mathbf{10}\% \rangle$	**Failure** $\langle \boldsymbol{f_{max}} \rangle$
Base case		0.1696	0.3924	0.5771	0.7893	0.8762	12.30
Case 1	EL	0.1969	0.3904	0.6129	0.7368	0.8903	14.02
Case 2	EL	0.2063	0.4480	0.6264	0.7917	0.8970	11.36
Case 3	EL	0.1901	0.4017	0.6123	0.7575	0.9292	11.16
Case 4	EL	0.1841	0.3946	0.5898	0.8081	0.9321	13.12
Case 5	EL	0.2008	0.3960	0.6355	0.7826	0.9537	12.22
Case 6	EL	0.1974	0.4101	0.6377	0.7353	0.9069	13.15
Case 7	EL	0.1808	0.3786	0.5944	0.8005	0.9085	14.52
Case 8	EL	0.1959	0.3978	0.6030	0.7780	0.8789	12.21
Case 9	EL	0.1739	0.4354	0.6183	0.7655	0.8992	11.71
Case 10	EL	0.1878	0.4002	0.6095	0.7981	0.8669	11.95
Case 11	EL	0.1833	0.3939	0.5580	0.7904	0.8828	13.32
Case 12	EL	0.1831	0.3779	0.6132	0.7852	0.8823	13.21
Case 13	EL	0.1879	0.3690	0.5883	0.7391	0.8434	13.25
Case 14	EL	0.1889	0.3739	0.5913	0.7904	0.9033	12.90
Case 15	EL	0.1910	0.4202	0.6072	0.8009	0.8978	13.24
Case 16	EL	0.1878	0.3747	0.6007	0.7640	0.9288	12.75
Case 17	EL	0.1935	0.4014	0.6019	0.7592	0.8562	13.86
Case 18	EL	0.1848	0.4400	0.6175	0.7610	0.8299	12.00
Case 19	EL+GL	0.1761	0.3808	0.5808	0.7503	0.8522	11.75
Case 20	EL	0.1900	0.3982	0.6225	0.7718	0.9014	12.38
Case 21	GL	0.2303	0.3856	0.5624	0.7652	0.8418	13.01
Case 22	GL	0.2003	0.3949	0.5667	0.7829	0.8232	11.34

Fig. 3 shows the geodesic vulnerability values ($\bar{v}$) for all the case studies corresponding to a loss of 10% of the nodes (*f*=10%). The trend line in Fig. 3 shows that the coupled system only improves when all the investments have been made (Case 22). The numerical values in Table I for (*f*=10%) demonstrate a 6% improvement in structural robustness, decreasing from a geodesic vulnerability value of 0.8762 to 0.8232 for Case 22 (taken from [31]).

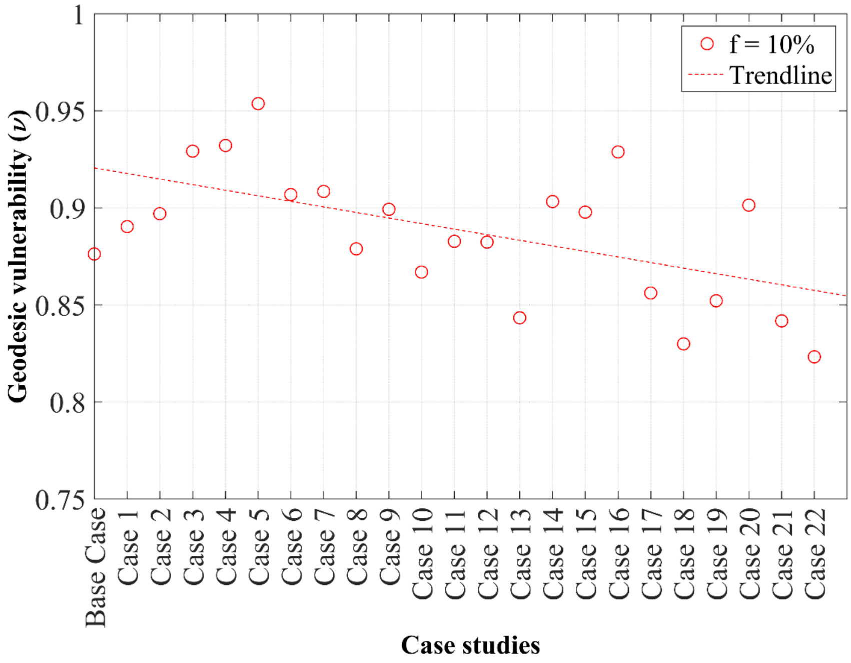


Figure 3. Geodesic vulnerability values for *f*=10% (taken from [31]).

6. Conclusions

The REDCRIT project developed a cascading failure methodology for coupled natural gas and electricity systems, remarkably simplifying the assessment of structural vulnerability using complex network theory. This proposal was previously validated in test networks and was applied here to real electricity and natural gas transmission networks in Spain. The results show that the natural gas system is less robust than the electrical system. In addition, the coupled network is more vulnerable than the electrical network to both random and deliberate faults, and the removal of 1% of the nodes is enough to completely collapse the network under intentional attacks on the infrastructure. Finally, the vulnerability of the system was evaluated with the construction of new power lines and gas pipelines between 2018 and 2020, resulting in a potential improvement of 6% in the combined robustness of the infrastructure.

Acknowledgements

This research was supported by the Ministerio de Economia y Competitividad (Ministry of Economy and Competitiveness), Spain, under project ENE2016-77172-R.

References

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

[2] Baldick, R., Chowdhury, B., Dobson, I. et al. (2009) Vulnerability assessment for cascading failures in electric power systems. *PSCE '09. IEEE/PES Power Systems Conference and Exposition* pp. 1-9.

[3] Brown, T. (2007) Multiple Modeling Approaches and Insights for Critical Infrastructure Protection." In: *IOS Press, NATO Series for Peace and Security Services. 13,* pp. 23-35.

[4] Barabási A-L, Albert R. (1999) Emergence of scaling in random networks, *Science*, 286, 509–12.

[5] Newman, M.E.J. (2003) The structure and function of complex networks. *SIAM Review*, 45, pp.167–256.

[6] Albert, R., Barabási, L. (2002) Statistical mechanics of complex networks. *Reviews of Modern Physics*, 74, pp. 47–97.

[7] Murray, A., Matisziw, T., Grubesic, T. (200/ Critical network infrastructure analysis: interdiction and system flow. *Journal of Geographical Systems*, 9, pp. 103–17.

[8] Motter, A., Lai, Y. (2002) Cascade-based attacks on complex networks. *Physical Review E*, 66, 065102.

[9] Crucitti, P., Latora, V., Marchiori, M., Rapisarda, A. (2004) Error and attack tolerance of complex networks. *Physica A: Statistical Mechanics and its Applications*, 340, pp. 388–94.

[10] Holmgren ÅJ. (2006) Using graph models to analyze the vulnerability of electric power networks. *Risk Analysis*, 26, pp. 955–69.

[11] Holmgren, ÅJ. (2007) A framework for vulnerability assessment of electric power systems. In: Murray AT, Grubesic TH, editors. *Critical infrastructure: reliability and vulnerability*. Berlin (Germany): Springer Verlag.

[12] Chen, G., Dong, Z.Y., Hill, D.J., Zhang, G.H. (2009) An improved model for structural vulnerability analysis of power networks. *Physica A*, 388, pp. 4259–66.

[13] Wang, K., Zhang, B., Zhang, Z., Yin, X., Wang, B. (2011) An electrical betweenness approach for vulnerability assessment of power grids considering the capacity of generators and load. *Physica A*, 390, pp. 4692–701.

[14] Jelenius, E. (2004) Graph models of infrastructures and the robustness of power grids. In: *Master thesis in physics engineering*. Stockholm (Sweden): Royal Institute of Technology (KTH).

[15] Solé, R., Casals, M., Murtra, B., Valverde, S. (2008) Robustness of the European power grids under intentional attack. *Physical Review E*, 77, 026102.

[16] Holmgren, A.J., Jenelius, E., Westin, J. (2007) Evaluating strategies for defending electric power networks against antagonistic attacks. *IEEE Transactions on Power Systems*, 22, pp. 76–84.

[17] Chen, G., Dong, Z.Y., Hill, D.J., Zhang, G.H., Hua, K.Q. (2010) Attack structural vulnerability of power grids: a hybrid approach based on complex networks. *Physica A: Statistical Mechanics and its Applications*, 389, pp. 595–603.

[18] Rinaldi, S.M., Peerenboom, J.P., Kelley, T.K. (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21 (6), pp. 11–25.

[19] McDaniels, T., Chang, S., Peterson, K., Mikawoz, J., Reed, D. (2007) Empirical framework for characterizing infrastructure failure interdependencies. *Journal of Infrastructure Systems.* 13 (3), pp. 175–184.

[20] Earl, E. et al. (2007) Restoration of services in interdependent infrastructure systems: a network flows approach. *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, 37 (6), pp. 1303–1317.

[21] Shahidehpour, M., Fu, Y., Wiedman, T. (2005) Impact of Natural Gas Infrastructure on Electric Power Systems, *Proceedings of the IEEE*, 93 (5)

[22] Urbina, M., Li, Z. (2008) Modeling and Analyzing the Impact of Interdependency between Natural Gas and Electricity Infrastructures. *IEEE Power and Energy Society General Meeting*.

[23] Cakir, B. et al. (2014) An integrated simulation model for analysing electricity and gas systems, *International Journal of Electrical Power and Energy Systems*, 61, pp. 410–420.

[24] Ouyang, M. (2014) Review on modeling and simulation of interdependent critical infrastructure systems, *Reliability Engineering and System Safety* 121, pp. 43–60.

[25] Wang S. et al. (2013) Analysis of interdependent infrastructure systems under edge attack strategies, *Safety Science*, 51 pp. 328–337.

[26] Correa, G.J., Yusta, J.M. (2013) Grid vulnerability analysis based on scale-free graphs versus power flow models, *Electric Power Systems Research,* vol. 101, pp. 71–79.

[27] Beyza, J., Yusta, J.M., Correa, G.J., Ruiz, H.F. (2018) Vulnerability assessment of a large electrical grid by new graph theory approach, *IEEE Latin America Transactions,*16, pp. 527–535.

[28] REE (2017) Spanish Electricity System 2017 Report. [Online]. Available: https://www.ree.es/en/statistical-data-of-spanish-electrical-system/annual-report/spanish-electricity-system-2017-report. [Accessed: 27-Nov-2018].

[29] Enagas (2018), Gas Transmission [Online]. Available: https://www.enagas.es/enagas/en/Transporte_de_gas/TransporteYOperacion/Transportista_de_gas_natural. [Accessed: 27-Nov-2018].

[30] Ministerio de Industria, Energia y Turismo, España (Ministry of Industry, Energy and Tourism, Spain). (2015) Planificacion Energetica. Plan de Desarrollo de la Red de Transporte de Energia Electrica 2015-2020

[31] Beyza, J., Yusta, J.M. (2018) Robustness Assessment of the Expansion of Coupled Electric Power and Natural Gas Networks Under Cascading Failures, *IET Generation, Transmission & Distribution*, Volume 12, Issue 21, 27 November 2018, p. 5753 – 5760.

Challenges to protect critical energy infrastructure

Vytis Kopustinskas[1]
European Commission, Joint Research Centre (JRC)
Directorate C - Energy, Transport and Climate
Energy Security, Distribution and Markets Unit
E. Fermi 2749, TP440, 21027 Ispra (VA), Italy

Marcelo Masera[2], Ricardo Bolado-Lavin[3]
European Commission, Joint Research Centre (JRC)
Directorate C - Energy, Transport and Climate
Energy Security, Distribution and Markets Unit
Westerduinweg 3, NL-1755 LE Petten, The Netherlands

Abstract

A wide plethora of traditional and emerging threats and hazards jeopardise the functioning of critical energy infrastructures. Hybrid threats, cyber and terrorist attacks, extreme climatic variations are among the more virulent. The regulatory environment needs to adapt to these changes, fostering the preparedness of society and the infrastructure operators. The European Commission has started discussions on the amendment of the Directive 2008/114/EC, which is in force since January 2009. The purpose of this paper is to discuss the main challenges in the area of critical energy infrastructure protection and the ways the policy might change.

Keywords: critical energy infrastructure, protection, energy security, security of supply, risk assessment.

1. Introduction

The Directive 2008/114/EC [1] is the result of work that started in 2004 when the European Council asked for the preparation of an overall strategy to protect critical infrastructures in the European Union. The Directive requested a step-by-step approach to identify and designate European Critical Infrastructures (ECIs). ECI is defined as a critical infrastructure located in one EU Member State whose disruption or destruction would have a significant impact on at least two EU Member States. The Directive takes into consideration the threat of terrorism, although it adopts a

[1] vytis.kopustinskas@ec.europa.eu

[2] marcelo.masera@ec.europa.eu

[3] ricardo.bolado-lavin@ec.europa.eu

general all-hazards approach. In the more than 10 years passed since the adoption of the Directive, it has become clear that a thorough consideration of all types of man–made intentional threats is required in the current geopolitical situation. In different settings, hybrid threats and cyber attacks are among the first to be mentioned.

The Directive in force specifically highlights the energy sector, with electricity, gas and oil subsectors as potential energy ECI. The other sector highlighted is the transport one, with road, rail, air, inland waterways transport, ocean and short sea shipping and ports as subsectors.

This paper focuses on the challenges faced by the critical energy infrastructure (CEI) protection domain.

2. The legislative background

The energy infrastructure regulation under Directive 2008/114/EC [1] is strongly interlinked with other regulatory documents for the electricity [2] and gas [3] subsectors, the EU energy strategy [4] and the Energy Union strategy [Ref]. The Energy Union consists of five closely related and mutually reinforcing dimensions:

- security, solidarity and trust: diversifying Europe's sources of energy and ensuring energy security through solidarity and cooperation between EU countries;
- a fully integrated internal energy market: enabling the free flow of energy through the EU through adequate infrastructure and without technical or regulatory barriers;
- energy efficiency: improved energy efficiency will reduce dependence on energy imports, lower emissions, and drive jobs and growth;
- decarbonising the economy: the EU is committed to a quick ratification of the Paris Agreement and to retaining its leadership in the area of renewable energy;
- research, innovation and competitiveness: supporting breakthroughs in low-carbon and clean energy technologies by prioritising research and innovation to drive the energy transition and improve competitiveness.

3. Challenges in critical energy infrastructure protection

In this chapter we will present the major challenges we see affecting CEI protection. We identify 4 major issues that need to be addressed:

- Identification of critical energy infrastructure;
- Capability to carry out complete risk assessment and consequence studies;
- Interpret and communicate quantitative and qualitative results of risk assessment;
- Exercising and planning.

3.1 Identification of the CEI

The major problem regarding the identification of a CEI relates to the fact that it might be cross-border – i.e. it can be located not only in one Member State, but also in more than two neighboring countries. This creates difficulties related to information access, regulatory framework and operational standards, especially during crisis situations. The regional aspect is crucial at the EU level for the identification of European critical infrastructures.

In our view, identification of the CEI should be based on methodological approaches, with a comprehensive all-hazard risk assessment as the basis. The method applied should identify:

- CEI assets whose disruption or destruction might have important local (one Member State) consequences;

- CEI assets whose disruption or destruction might have important regional (two or more Member States) consequences.

The latter is defined as ECI in the Directive [1]. It is obvious that a risk assessment performed for the identification of ECI should include a number of Member States, covering the region relevant for analysing the given infrastructure. If needed, the analysis could be split into several regions, including overlapping among themselves when so required.

The regional approach is also enforced in the EU Regulation [3] for gas supply and in the new EU Regulation for electricity supply [5]. Both regulations also promote the solidarity principle of sharing resources in case of crisis, however their operational implementation still needs to be further detailed.

Another issue is the protection of the identified CEI assets. Among other measures, this is ensured by the development of preparedness and emergency plans. Both type of plans are challenged in case of cross-border ECI assets.

The preparedness action plan has to allocate limited resources to different risks avoiding "waiting until event happens" situation. However, both the allocation of costs and responsibilities to cross-border infrastructure, and the development of coordination mechanisms are not straightforward tasks.

Similar challenges are foreseen for the development of emergency plans. As an emergency plan for a single Member State often relies on optimistic assumptions about possible supply from another Member State, regional emergency plans should be considered. Crisis preparedness and cross-border coordination must be effectively implemented, as crisis almost always evolves under time pressure.

3.2 Capability to carry out complete risk assessment and consequence studies

The first challenge of identification of CEI should be based on a comprehensive risk assessment based on an all-hazard and all-threat approach at the regional scale. It should address:

- Natural hazards;
- Technological hazards and equipment failures;
- Intentional man-made threats: cyber-attacks, hybrid attacks, insider sabotage, antagonist/terrorist actions;
- Interdependencies among CEIs, cascading effects within one CEI and across several CEIs;
- Single supply source evaluation.

The consequences of hazards and threats should be evaluated regarding their impact on vital societal functions of one or several Member States. Currently, many studies end up with estimation of non-supply volumes, and the impact evaluation on societal functions is missing.

There is a need to harmonise assessment approaches at the EU level taking into account the state of the art in Europe and worldwide.

3.3 Interpret and communicate quantitative and qualitative results of risk assessment

Many hazards listed in the section above and treated in the framework of classical risk assessment can be assessed quantitatively with methods described in the literature. However many emerging threats, especially intentional and well planned attacks, in which damage of CEI might be only a partial goal, followed by e.g. fake news background in the media or military and hybrid actions, are difficult to analyse quantitatively and often rely on qualitative evaluation and assessment.

The all-hazard and all-threat approach to risk assessment requires then to merge the results of quantitative and qualitative analysis to obtain a single risk measure and to communicate it to public, policy makers and stakeholders. Having a single risk metrics allowing prioritisation and ranking of the main risk contributors is important if one wishes to develop an optimal framework to distribute limited resources for risk mitigation.

The issue is even more complicated when dealing with cross-border CEIs, involving different languages, approaches, definitions and legal frameworks.

3.4 Exercising and planning

The last challenge we identify is related to exercising, planning and learning. Real and big crisis are rare and we cannot afford to only learn from past crisis events. There must be a continuous procedure to test the emergency and preparedness plans by means of tabletop and field exercises, continuous updating of risk assessments by implementing a living risk assessment approach following the evolution of the infrastructure, consumer behaviors, natural hazards and the emergence of new threats.

The future planning and development of the infrastructure should be based on the outcome of comprehensive regional risk assessment studies.

Continuous updating is needed not only at the analysis level, but also at regulatory level. The gas supply regulation has been recently updated, the new electricity regulation is expected to enter into force in 2019 and preparations have started for a new Directive on critical infrastructure protection.

4. Concluding remarks

The paper describes a number of challenges we consider as the most important for further development of critical energy infrastructure protection, especially with a view of upcoming revision of the Directive [1]. Below we list the main areas of challenges for critical energy infrastructure protection:

- Identification of CEI (critical nodes and facilities) considering cross-border importance and interdependency;
- Capability to carry out comprehensive risk assessment and consequence studies
- Interpret and communicate quantitative and qualitative results of risk assessment
- Exercising and planning

All these challenges are underpinned by the fact that some CEIs are located in several Member States or are located in one, but strongly affect the other. There is a strong need for regional approaches involving several Member States in many steps of CEI design, planning, operation, exercising and crisis management. The cross-border infrastructure issues are also challenged by different legal frameworks, operational standards, different spoken languages and approaches to crisis management.

A special attention should be given to full scope risk assessment capabilities, as CEI as interdependent, cascading effects are likely to evolve during large crisis and intentional threats might be difficult to identify and diagnose right from the beginning of crisis.

References

[1] Directive 2008/114/EC (2008). Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union, L 345/81, Luxembourg.

[2] Directive 2005/89/EC (2006). Directive 2005/89/EC of the European Parliament and of the Council of 18 January 2006 concerning measures to safeguard security of electricity supply and infrastructure investment. Official Journal of the European Union, L33/22, Luxembourg.

[3] EU Regulation (2017) Regulation 2017/1938 of the European Parliament and of the Council of 25 October 2017 concerning measures to safeguard the security of gas supply and repealing Regulation (EU) No 994/2010. Official Journal of the European Union, L280/1, Luxembourg.

[4] European Energy Security Strategy (2014). Communication from the Commission to the European Parliament and the Council. COM(2014) 330 final. Brussels, Belgium.

[5] Proposal for a Regulation of the European Parliament and of the Council on risk-preparedness in the electricity sector and repealing Directive 2005/89/EC, COM(2016) 862 final, Brussels.

Analysis of the impact of the Asset Health Index in a Maintenance Strategy

Javier Serra
Asset Management Technician, Enagas
Paseo de los Omos 19
28005, Madrid, Spain

Adolfo Crespo, Juan Gómez
University of Seville, Spain

Antonio Sola
Ingeman, Spain

Abstract

During many years, asset management methodologies used in industry were focused on knowing and analysing the operational control of the daily work and the impact of the maintenance on the availability. Later, the costs turn into the priority, and strategies were focused on assesses a longer lifecycle and optimizing processes and contracts. Finally, recent normative have included concepts as "knowing and managing the risks" and the target is to prioritize the maintenance tasks to the critical assets. However, taking a balanced asset management model for the operational environment, quite a lot of facilities of Oil & Gas sector are reaching the end of their initially estimated lifecycle. New challenges are related to extend the life of the main items of the facilities or at least, to find the optimal replacement moment that guarantees that the maintenance strategy is being optimized.

Asset Health Index methodology considers a theoretical lifecycle of an item, in which depending on the proximity to the end of the useful life, the probability of failure increases. But take this theoretical lifecycle as a base, different operation location factors or O&M aspects can modify this period. All these factor are quantified and permit us to calculate a new theoretical profile.

This paper is about assess the impact of the AHI into the maintenance strategy optimisation. AHI enables us to compare future alternative cost profiles and assess the impact in the failure probability of the item. As a result, we are able to know the risk that is taken when we enlarge the operation of an item, and the impact in the operational costs.

Keywords: Asset Management, Maintenance strategies, lifecycle, Asset condition

1. Introduction

The target of the paper is to assess the profitability of the investment in a replacement asset process. Traditional profitability analysis takes into account standard Opex and Capex concepts. However, when these studies are made for long term investments or for long time periods, the evolution of these costs are not always well defined.

Some concepts are easy to calculate because they have a lineal or non-variable evolution. If the asset technology is well known, electricity consumption or CO2 emission is a direct calculation. On the other hand, costs derived from the ageing of the assets as corrective maintenance does not have a clear methodology to be calculated.

Asset Health Index provides an objective technical methodology to estimate the lifecycle bend and, in consequence, maintenance cost profiles in the future. This estimation enable us to use reliability index as availability in the investment study. Capex and Opex have been traditionally used separately because were focused on specific targets; Capex for making the best investment, and Opex for reaching operational efficiency. However, developing methodologies that are focused on TOTEX guarantees the effectiveness of the asset management in long term results.

2. Scope

2.1 Definition

An Underground Storage of Natural Gas is used to store NG in low consumption periods (e.g. summer) and be able to use it in consumption peaks (e.g. winter). In the extraction process, natural gas flows mixed with water and other condensed products which are taken from the ground. To avoid mixing these products with the Gas Transport Grid, it is necessary to cool the gas. Water and impurities get condensed and can be eliminated. After that, natural gas get the right levels of water and hydrocarbons required by the law.

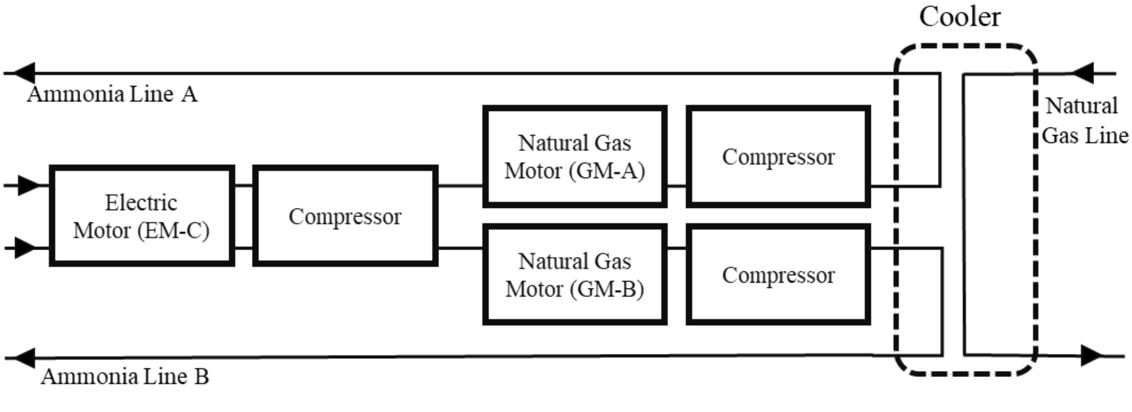


Figure 1. Basic System Diagram

NG is cooled by two refrigeration lines whose refrigerant fluid is ammonia. This fluid must be compressed to maintain the heat exchange with NG. Three compressors are used for this process. These compressors are actuated for three motors of different technologies. Two natural gas motors used for compressors of line A and Line B, and a third electric compressor that can operate for both lines. The basic system diagram is shown in Figure 1.

As a result of the experience of the staff of the facility operating and maintaining the motors, it is proposed to change one of the natural gas motors for an electric one. It will avoid the CO2 emitted in the natural gas combustion and will optimise OPEX during the lifecycle of the item.

The target of the paper is to calculate the profitability analysis of the change, assessing the impact of the Health Index of the motors in the operation and maintenance costs. This methodology allows to estimate the impact of the ageing of an asset during the lifecycle.

2.2 Operation scenarios

According to the configuration of the system, electric compressor (EM-C) was used just as a backup of the natural gas ones.

As a result of the benefits of using the electrical motor the last year, the operating process time was divided at 50% for the electrical one and 50% for natural gas ones (25% for each one) as shown in Figure 2.

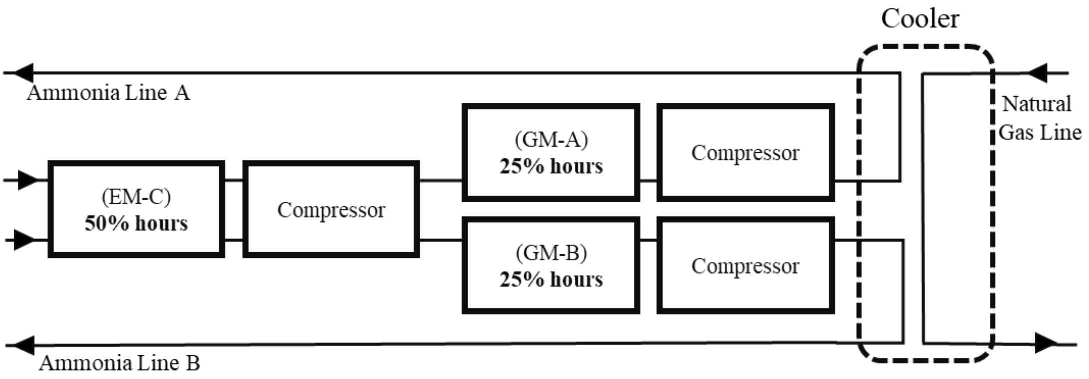


Figure 2. Current Operational mode

To maximize the benefits of the investment, the calculation is not only going to be based on the change of technology (GM-A for EM-D) but on the change of the operational mode. The scenario proposed uses electrical motors as main equipment, letting the natural gas one as backup. It implies that actual EM-C will work 50% of the time, and preferably on line B. On the other hand, the new EM-D will be used the other 50% of the time, and can only work on line A. The new scenario is shown on Figure 3.

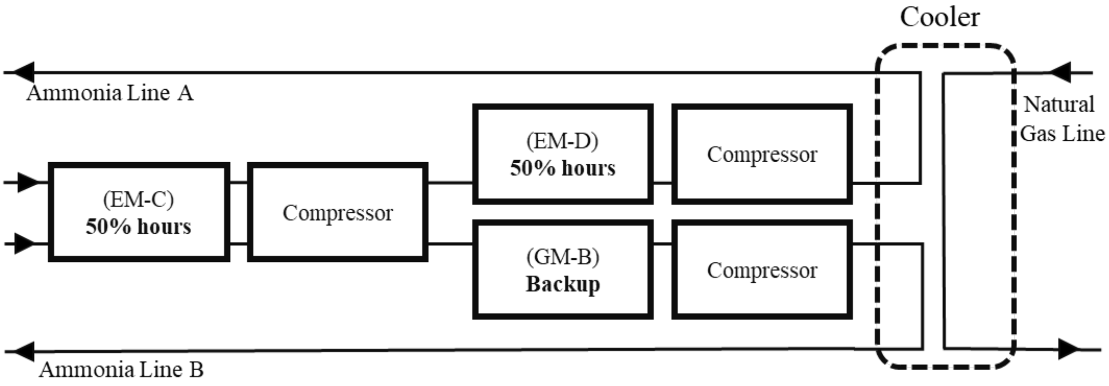


Figure 3. Proposal of new operational mode

This proposal has several benefits that are going to have impact in the payback of the investment:

- Improving the energy efficiency; electrical motors has better efficiency rates during the operation so it is assumed to be an optimised use of energy.
- Decreasing CO2 emissions; avoiding the use of natural gas as energy for the NG motors can decrease significantly emissions of gases derived of combustion process.
- Increasing reliability of the facility; failure rates of electric motors are significantly lower than NG ones. This factor increases the availability level of the facility.
- Optimising maintenance costs; electric motors does not require overhauls, so the scheduled availability increases against NG motors.
- Decrease the criticality of the asset; according to the criticality analysis, [1][2] Natural Gas Motors are more critical because of the environmental care impact. The change of technology decrease the criticality of the asset, and consequently provides the facility more flexibility in maintenance plans optimising processes.

3. Asset Health Index Calculation

Asset Health Index (AHI) represent a practical methodology to quantify the general health of a complex asset. [3]. The methodology is used to provide a mathematical base for supporting maintenance and replacement strategies. The index represent the asset conditioned based on a semi quantitative assessment of the factors that impact in the lifecycle of an item. With the assessment of the impact of the factors, we can use the results of operational observations, field inspections and laboratory tests, to simulate the lifecycle of an asset [4]. This estimation must help to know the future condition, and consequently the costs derived from the operation and maintenance.

In this case, the methodology is going to be applied in the NG motor (GM-A). It is supposed that the electrical one is a new asset and the wear and tear during the period of the analysis is not going to be relevant, so is not going to have impact into the global maintenance costs.

3.1 Background

The asset health index (AHI) is considered as a dimensionless number between 0.5 (which corresponds to its status or condition as new equipment) and the value of 10 (corresponding to the condition of the equipment at the end of its useful life). The behaviour pattern of the AHI, is supposed to be exponential along the age of the asset. The Figure 4 shows the different five sections into which the health index of the asset is divided [5].

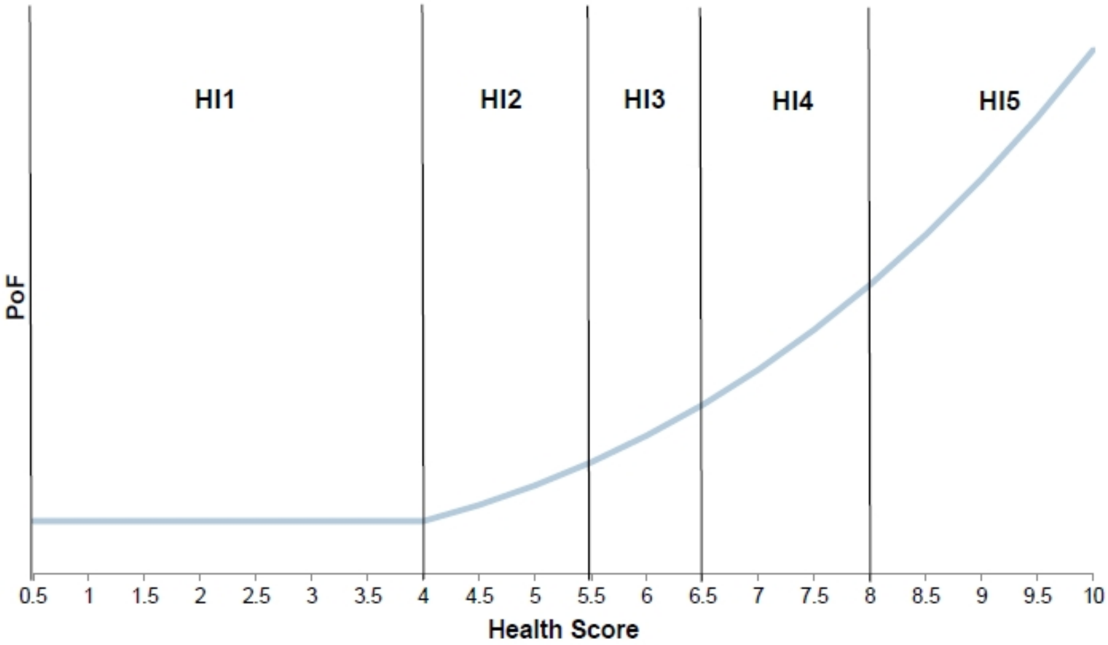


Figure 4. Asset Health Index Banding

The HI1 range comprised 0.5≤AHI≤4 values; for which the behavior of the equipment is assumed to resemble as new equipment. The HI2 range considers AHI values within the interval 4<AHI≤6 and corresponds to the period of time when the first signs of deterioration begin to appear in the equipment. In this range, the value corresponding to AHI=5.5, is assumed to be the health index value equivalent to the normal life expected for the equipment category. From this point, three intervals are considered in the methodology: HI3, HI4 and HI5 as the AHI exceeds the values of 6, 7 and 8 respectively. The methodology assumes that exceeded the value of AHI=8, the equipment is at the end of its useful life. Due to the workshop nature of ESReDA Seminars, strict rules about paper length are not imposed on authors. However we recommend that the paper be of maximum 12 pages in length. Please use these guidelines when writing your paper. By following them carefully you will contribute to reducing the time needed to issue the proceedings.

3.2 Procedure

The methodology followed in this paper is based on a procedure consisting in five consecutive steps [6]. Taking the theoretical estimated normal life based on the provider information and associate with a specific equipment category, several factors update this expected life. Every aspect related with the asset condition is taken into account and used in the methodology. This procedure is presented in Figure 5.

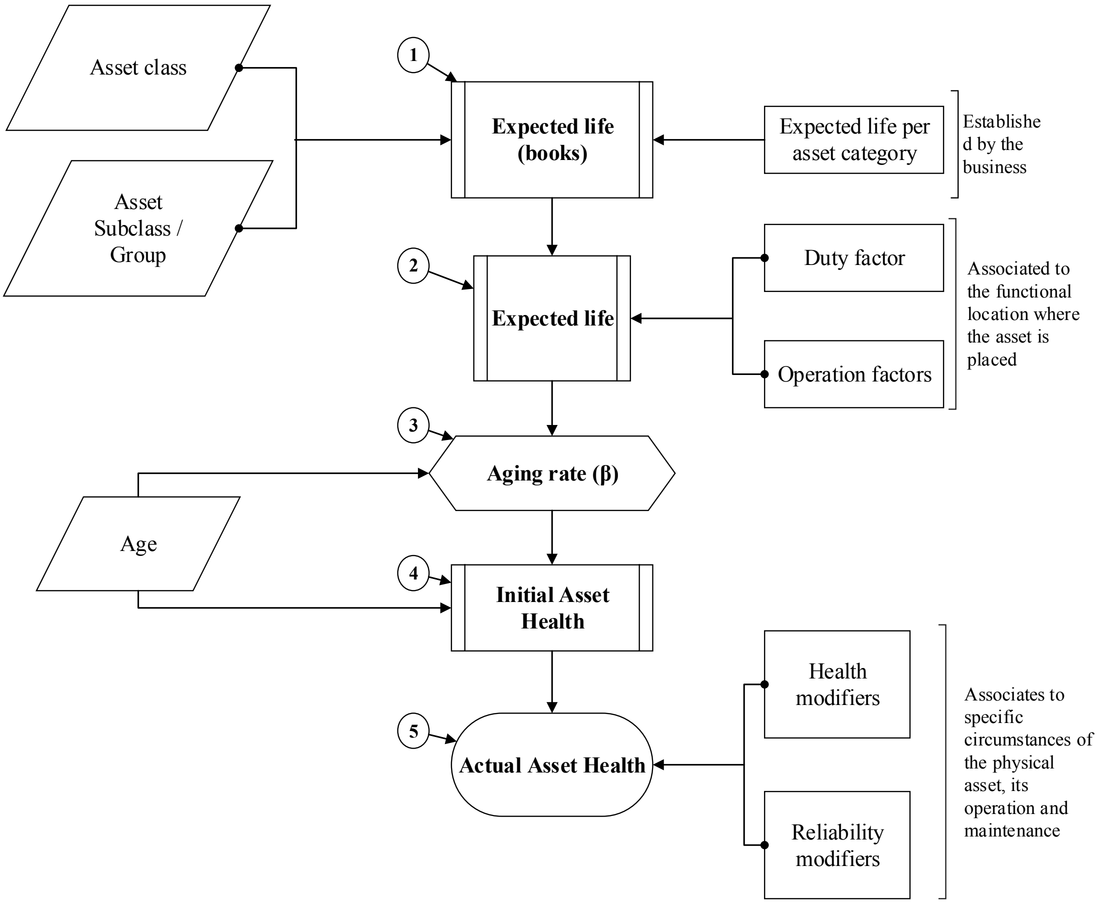

Asset class
Asset Subclass / Group
Age
1
Expected life (books)
Expected life per asset category
Established by the business
2
Expected life
Duty factor
Operation factors
Associated to the functional location where the asset is placed
3
Aging rate (β)
4
Initial Asset Health
5
Actual Asset Health
Health modifiers
Reliability modifiers
Associates to specific circumstances of the physical asset, its operation and maintenance

Figure 5. AHI Calculation Procedure

Using the theoretical procedure proposed [6], the practical application is going to be explained with the case study of NG motor (GM-A) following the five steps define previously.

3.2.1 Asset selection and category definition: In this first step, the identification of the asset and all the information regarding its functional location is addressed. According to ISO 14224 the asset is included in rotating equipment category and the equipment class is known as “electric motors”.

3.2.2 Evaluation of the impact of location and load factors: Once all the information in the previous point has been compiled, the location and loading factors are

evaluated. This step will quantify the impact of the specific place of the asset, and the load conditions derived of it, into the expected life.
To calculate location factor (F_LT), reference standards as DNO common network asset indices methodology proposes collections of factors, but these must be adapted to the type of facility and operational process. Location factors proposed for Underground Gas Storage are defined in Table 1, Table 2 and Table 3. The range and the value of the factors have been defined based on the experience and knowledge of the staff of the facility. The range that applies for GM-A is marked in grey.

Table I: Location Factor; Distance to coast

Distance to coast (km)	**Factor Value**
0 Km – 1 Km	1
1 Km – 5 Km	1.05
5 Km – 10 Km	1.1
10 Km – 20 Km	1.15
> 20 Km	1.2

Table II: Location Factor; Outside Temperature

Temperature (ºC)	**Factor Value**
0 ºC – 10 ºC	1
10 ºC – 20 ºC	1.1
20 ºC – 30 ºC	1.2
> 30 ºC	1.3

Table III: Location Factor; Height above sea level

Height (m)	**Factor Value**
0 – 500	1
500 – 1000	1.1
1000 – 2000	1.2
> 2000	1.3

If there are several parameters that impacts in location factor calculation, the methodology defines that

$$F_{LT} = max(F_{LT1}, F_{LT2}, F_{LTx}) \quad (1)$$

In this case, the first location factor (F_{LT1}) is distance to coast and the facility is off-shore, so the distance is 0 km and the factor value is 1. The second factor (F_{LT2}) is outside temperature. The average value is 21ºC throughout the year so the factor value according to the Table 2 is 1.1. Finally, the height above sea also conditioned the expected life of the asset. In this case the facility is at sea level and the factor value is 1. As a consequence, the Location Factor is 1.1 as shown in equation 2:

$$F_{LT} = max(1,1.1,1) \quad (2)$$

To calculate load factor (F_L) it is necessary to measure the load requested during operation in the specific location against the maximum admissible load measured during the start-up process of the equipment.

$$F_L = \frac{Load\ normal\ conditions}{Maximum\ admissible\ load} \qquad (3)$$

After running test, the load measure for nominal conditions is 90% of maximum admissible. In this case, the load factor (F_L) is 0,9. According to the methodology we can now calculate a new estimate life as a result of the equation

$$Estimated\ life = \frac{Normal\ life}{F_{TL} \times F_L} \qquad (4)$$

The normal life defined by the provider is 25000 hours. It is the operation time until the overhaul must be done. Consequently, is the expected life noted by the provider in which the failure rate is the standard one, so the AHI is under 5.5.

According to the evaluation of the impact and the location, the estimated life is higher and is expected to be under the standard failure rate until 25253 operation hours.

<u>3.2.3 Calculation of the aging rate:</u> A fundamental hypothesis of the chosen methodology is that the aging of an asset has an exponential behaviour with respect to its age. This aging can be calculated through the parameter aging rate, and permit us to use this rate for express mathematically the behaviour of failure rate during the lifecycle.

The calculation is

$$\beta = \frac{\ln \frac{HI_{new}}{HI_{estimated\ life}}}{Estimated\ life} \qquad (5)$$

Where:

β = Aging rate.

HI_{new} = 0.5 Health index corresponding to a new asset;

$HI_{estimated\ life}$ = 5.5 Health index corresponding to an asset arriving to its estimated life;

<u>3.2.4 Obtaining the Initial Health Index:</u> After calculating the aging rate, we are able to obtain the Initial Health Index. This new Index represents an adaptation of the theoretical provider expected life into a new real expected life condition by the specific installation place (defined by location factors) and with a specific load condition (defined by the load factor). As a result, we obtain a graphical result shown in Figure 6.

$$HI_i = HI_{new} x e^{\beta t} \qquad (6)$$

Where:

t = the current age of the asset (in units of time)

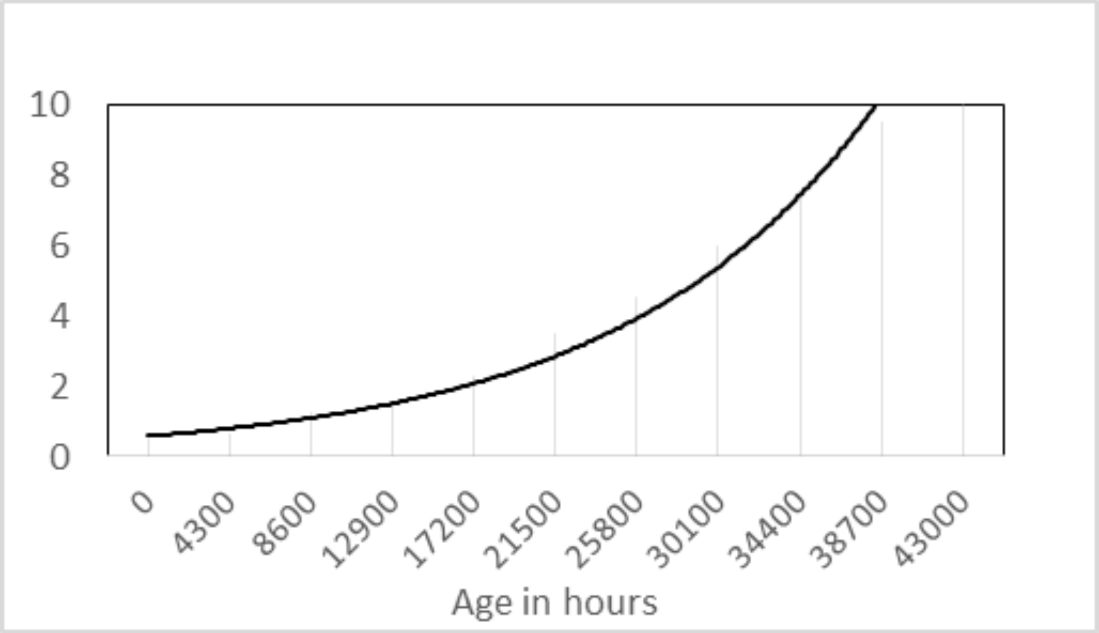


Figure 6. Initial Health Index

<u>3.2.5 Calculation of the Real Health Index:</u> In the last step, the aging of the asset can be increased or decreased by other modifiers that conditioned the operation and the maintenance. These factors are divided into three categories; reliability, load and healthy modifiers.

Reliability modifiers are shown in Table 4, Table 5 and Table 6, and represents the results of the operation rules of the asset:

Table IV: Reliability Modifier; Inactivity Operating Time

Inactivity (%)	Modifier Value
0 % – 50 %	1
50 % – 75 %	1.05
75 % – 100 %	1.1

Table V: Reliability Modifier; Provider

Provider (average reliabity)	Modifier Value
Under range average providers	1.05
Into range average providers	1
Upper range average providers	1.05

Table VI: Reliability Modifier; Overhauls number

Overhauls (number)	Modifier Value
1-3	1
3-5	1.05
>5	1.1

The healthy modifier is shown in Table 7 and quantify the impact of the specific operation parameter into the lifecycle of the asset. In this case the continuous start-ups of the machine:

Table VII: Health Modifier; Number of start-ups

Start-ups (number)	Modifier Value
< 40	1
40 < x < 80	1.2
80 < x < 120	1.4
> 120	1.6

Finally, operating an asset out of load range can modify the expected life, and it must be represented by AHI. In this case it is represented in load modifier (Table 8).

Table VIII: Load Modifier; Operating Load

Average Operation Load	Modifier Value
Into the recommended range	1
0% < X < 15% out of range	1.3
15% < X < 30% out of range	1.5

The result of the process is shown in Figure 7 and includes the comparison between the initial health index and the current health index.

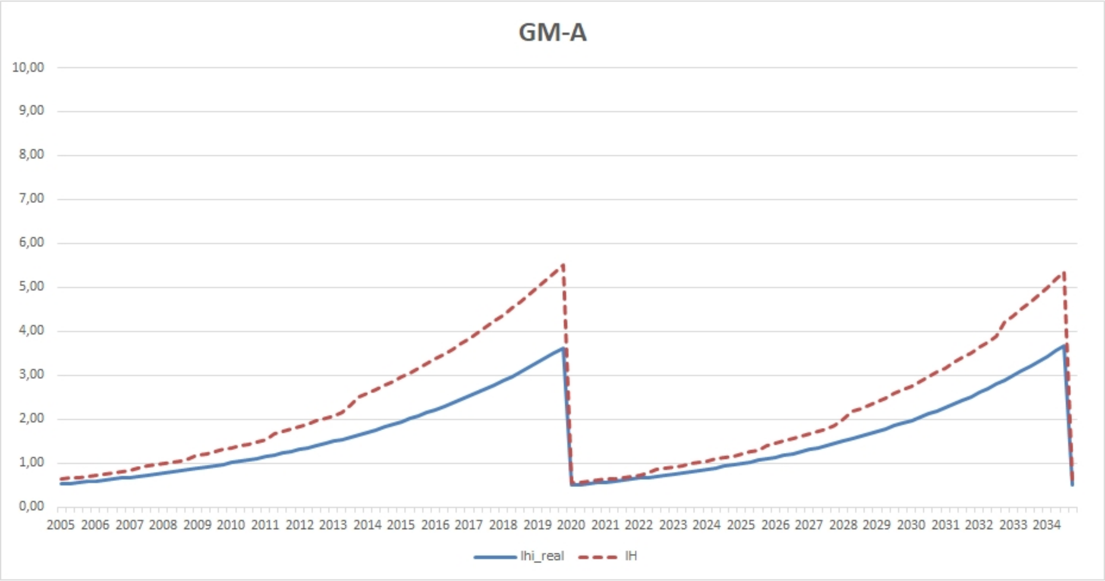


Figure 7. HI initial vs HI real

Having defined all the parameters, and calculated all the factors, we can finally obtain the Real Health Index(HI_r). This value shows the most objective estimation of the age of an asset. It is calculated according to the next equation:

$$HI_r = HI_{new} \frac{\beta t}{e^{M_L}} \; x \; M_H \; x \; M_R \qquad (7)$$

Where:

M_L = Load Modifier

M_H = Healthy Modifier

M_R = Reliability Modifier

3.3 AHI Results

Depending on the design of the model, and the values of the modifiers, the Health Index, and consequently, the lifecycle, can be increased or decreased against the theoretical proposed by the provider. These results can be used as a base for management decisions (Table 9). Knowing the factors that impact in the health and calculating the HI, allow us to prevent premature aging and advance maintenance tasks. On the other hand, it also allows us to optimise operation and extending the life of the asset. With this information, we can adjust the maintenance plan and optimise the OPEX.

The results of the AHI calculated for motor (GM-A) shows that, because of the operation mode of the motor, its lifecycle is being shortened. According to the Health Index, the overhaul must be made in advance of at least two years. The Health Index in 2019 will reach 5.5, which is the moment when the failure rate can increase and consequently, impact into the reliability of the asset. This overhaul in advance, causes that in the period used for profitability calculation (15 years) two overhauls must be made instead of one. This change impacts directly in the economical result.

Table IX: Load Modifier; Operating Load

AHI	Condition	Expected lifetime	Requirements
0.5 - 4	Very good	>5 years	Normal maintenance
4 – 5.5	Good	> 4 years	Normal maintenance
6 - 7	Fair	2 – 3 years	Increase diagnostic
7 - 8	Poor	< 2 years	Planning replacing
8 - 10	Very poor	End of life	Immediately replace

4. Profitability Calculation

4.1 Considerations

To analyse the impact of the lifecycle maintenance cost of the motors into the profitability calculation, Internal Rate of Return (IRR) has been used as the main indicator to assess the benefits of the investment. To simplify the analysis and avoid unnecessary data, there have not been included all parameters that do not change between the scenarios that are going to be compared (replacing GM-A by EM-D or keeping it on GM-A).

4.1.1 Operational considerations: the operation parameters considered for the investment assessment are the energy consumption of the motors (natural gas for

GM-A and GM-B or electricity for EM-C and EM-D) and the CO2 emitted in the natural gas combustion.

The operation scenario has been defined previously. To maximize the hypothetical benefits of the replacement, the proposal is not just to change the motors but to use electrical ones as the main equipment and leave the second natural gas motor (GM-B) as backup item. As a consequence, it is necessary to consider not just the energy savings of GM-A, but adding GM-B. In the assessment we have consider a 90% of operational savings in GM-B. 10% of the operation time is maintained, considering the hypothetical backup operation of the motor, and the time used for periodical maintenance start-ups.

According to the previous consideration, CO2 emissions have been calculated estimating a total saving of GM-A emissions and a 90% of GM-B emissions.

4.1.2 Maintenance considerations: maintenance costs have been simplified into two concepts to simplify the assessment. Firstly, the general maintenance costs which includes periodical preventive maintenance and standard corrective maintenance (derived from the average failure rate). Based on AHI value, asset condition is supposed to be under 5.5, so corrective standard costs are fixed during the lifecycle. Secondly, the overhaul, which includes the major maintenance if it is required. In this case, this overhaul is just necessary for NG motors, and this factor is going to be critical in the calculation of profitability. Overtaking or delaying overhauls has a direct impact in the costs of the lifecycle.

4.1.3 Price considerations: To complete the analysis, it is necessary to take parameter prices as reference. All prices has been estimated with the recommendation of the specifics specialist departments of the company. However, for the business profitability calculation, parameters as CO2 ton or electricity has very variable prices and the margin of uncertainty is important. In this case, for the theoretical demonstration of the impact in the lifecycle, these prices have been considered fixed. The price used for electricity is 0,07€/kWh and for CO2 is 9,55€/Ton. The IRR calculation requires also use specific economical parameters. The three economic factors considered have been; the discount rate (25%), the increase of consumer price index (2%) and the investment amortization period (15 years)

4.1.4 Investment considerations: To complete the comparison of the changing of the motor, it is necessary to include the costs needed for the installation of the new asset. In this concept are included all the costs; the asset, works necessaries for the installation, facility adaptation to new asset, engineering work hours, disassembly old equipment and control system modification. The value or these costs is 340k€.

4.2 Calculation of Internal Rate of Return

To approve investment proposals, companies requires a clear profitability value. The key performance indicator to assess this viability is the Internal Rate of Return. The value required depends on the company. In most cases, no investment is approved with values lower than 6% (a standard value of the Return Rate just for investing in the bank). The higher the IRR, the greater the probability the investment was approved.

To analyse the IRR, a standard spreadsheet has been used. Costs savings derived from the replacement of NG motor has been considered with positive value. In Table 10 are detailed direct costs of operation and maintenance of GM-A which are going to be eliminated because of the replacement:

Table X: Cost Savings; GM-A

Concept	Asset	Value (k€)	Periodicity
Overhaul	GM-A	140	25.000 h
Maintenance	GM-A	10	Annual
Natural Gas	GM-A	30	Annual
CO2 emissions	GM-A	1,83	Annual

As it has been explained previously, it is also considered the savings derived from the operational change mode. It implies a 90% reduction of annual costs, and not taking into account a hypothetical overhaul of GM-B, because the operational hours will not reach 25.000 hours during the investment calculation. The detail is shown in Table 11.

Table XI: Cost Savings; GM-B

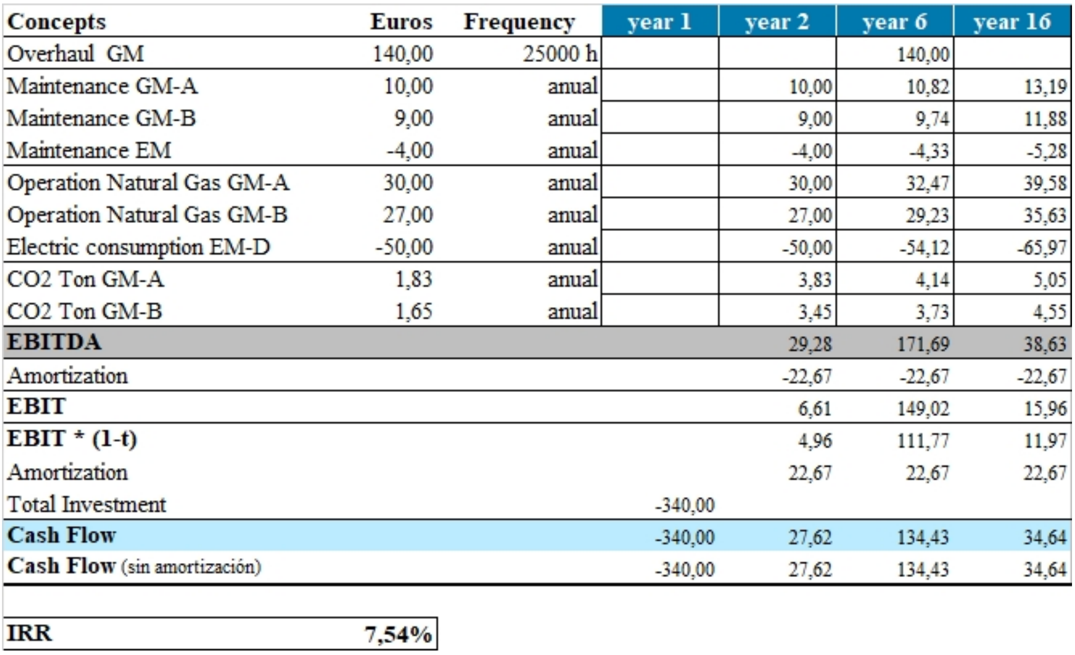
Concept	Asset	Value (k€)	Periodicity
Overhaul	GM-B	140	Not used
Maintenance	GM-B	9	Annual
Natural Gas	GM-B	27	Annual
CO2 emissions	GM-B	1,65	Annual

New costs derived from the installation of the EM-D, has been considered in the spreadsheet with negative value and are detailed in Table 12.

Table XII: Cost Increase

Concept	Asset	Value (k€)	Periodicity
Overhaul EM	EM-D	0	Not applied
Maintenance	EM-D	4	Annual
Electricity	EM-D	50	Annual

4.2.1 Calculation without AHI: If the assessment was done without including AHI concept, the calculation was normal. The only singular point would be to estimate when is going to be the overhaul done. Assuming annual operation hours defined in the base case, there will be necessary just one overhaul during the lifecycle of the investment (15 years) which might be done in the fifth year of the cycle (according to the actual situation of the asset). Using standard data into the spreadsheet and with the considerations defined along the paper, the IRR will be 7.54%. Figure 8 represents a simplified image of the spreadsheet. It includes the first year (moment of the hypothetical investment), the second year (that is the example for the rest the years) and the year where the overhaul is going to be executed.

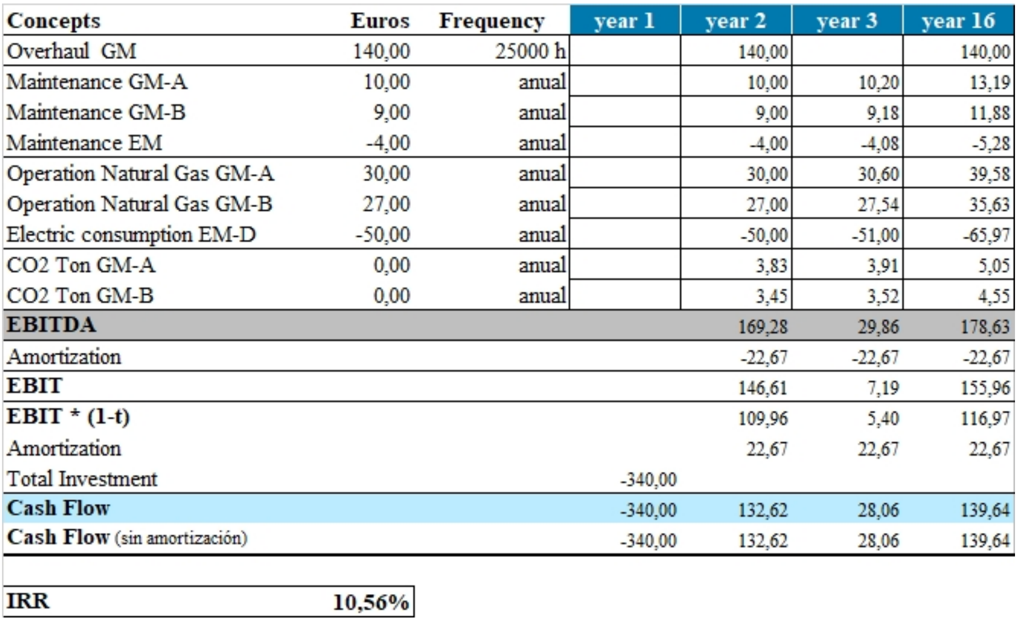


Concepts	Euros	Frequency	year 1	year 2	year 6	year 16
Overhaul GM	140,00	25000 h			140,00	
Maintenance GM-A	10,00	anual		10,00	10,82	13,19
Maintenance GM-B	9,00	anual		9,00	9,74	11,88
Maintenance EM	-4,00	anual		-4,00	-4,33	-5,28
Operation Natural Gas GM-A	30,00	anual		30,00	32,47	39,58
Operation Natural Gas GM-B	27,00	anual		27,00	29,23	35,63
Electric consumption EM-D	-50,00	anual		-50,00	-54,12	-65,97
CO2 Ton GM-A	1,83	anual		3,83	4,14	5,05
CO2 Ton GM-B	1,65	anual		3,45	3,73	4,55
EBITDA				29,28	171,69	38,63
Amortization				-22,67	-22,67	-22,67
EBIT				6,61	149,02	15,96
EBIT * (1-t)				4,96	111,77	11,97
Amortization				22,67	22,67	22,67
Total Investment			-340,00			
Cash Flow			-340,00	27,62	134,43	34,64
Cash Flow (sin amortización)			-340,00	27,62	134,43	34,64

IRR	**7,54%**

Figure 8. IRR spreadsheet without HI

<u>4.2.2 Calculation with AHI:</u> When the assessment is done taking into account AHI, some key aspects change significantly. The curve that represents HI_r(Figure 7) demonstrate that the asset condition is worse than expected for current working hours. The factor that have more influence in the wear and tear is the healthy modifier. It results in major maintenance being advanced four years. Even a second overhaul must be done into the analysis period. With these data included in the spreadsheet (Figure 9), IRR changes significantly, increasing the value until 10,56%.



Concepts	Euros	Frequency	year 1	year 2	year 3	year 16
Overhaul GM	140,00	25000 h		140,00		140,00
Maintenance GM-A	10,00	anual		10,00	10,20	13,19
Maintenance GM-B	9,00	anual		9,00	9,18	11,88
Maintenance EM	-4,00	anual		-4,00	-4,08	-5,28
Operation Natural Gas GM-A	30,00	anual		30,00	30,60	39,58
Operation Natural Gas GM-B	27,00	anual		27,00	27,54	35,63
Electric consumption EM-D	-50,00	anual		-50,00	-51,00	-65,97
CO2 Ton GM-A	0,00	anual		3,83	3,91	5,05
CO2 Ton GM-B	0,00	anual		3,45	3,52	4,55
EBITDA				169,28	29,86	178,63
Amortization				-22,67	-22,67	-22,67
EBIT				146,61	7,19	155,96
EBIT * (1-t)				109,96	5,40	116,97
Amortization				22,67	22,67	22,67
Total Investment			-340,00			
Cash Flow			-340,00	132,62	28,06	139,64
Cash Flow (sin amortización)			-340,00	132,62	28,06	139,64

IRR	**10,56%**

Figure 9. IRR spreadsheet with HI

5. Conclusion

The use of the methodology of AHI for the profitability calculation has had a deep impact. It has conditioned significantly the maintenance strategy during the lifecycle of the investment.

It is not only the final 4% of difference in the IRR between the calculations without AHI against the one with AHI. The reason that make the investment more realistic, is the knowledge of the real status of the asset. This knowledge enables us to turn a subjective assessment of asset condition into a mathematical calculation

The application of the methodology allows us to know that the operational mode of the Gas Motor has decreased significantly its lifecycle. Assuming the information given by the provider, it could be possible to reach 25.000 operation hours. And this scenario is not necessaryly wrong. The AHI allow us to determine the risk that it is being assumed by waiting until the overhaul. Or even if it is possible, to advance this major maintenance, ensuring that the asset condition is good enough.

In a business profitability assessment, non-lineal costs are the values most difficult to estimate. Especially when the asset is reaching the end of the useful life, it is difficult to quantify the increase of the costs derived from the wear and tear.

Finally, is also important to remark that one of the most valuable aspects of a semi quantitative methodology, is the knowledge management. In this paper all the parameters of the procedure (modifiers, factors…) are assumed. But the process of obtaining the necessary agreements by the specialist, implies to sharing the knowledge, and recording deliverables. For companies with specialists with more than 40 years of experience, this process helps to prepare better the future of the business.

6. References

[1] Crespo Márquez, Adolfo; Moreu de Leon, Pedro; Sola Rosique, Antonio; Gómez Fernández, Juan Francisco. Criticality Analysis for Maintenance Purposes: A Study for Complex In-service Engineering Assets. En: Quality and Reliability Engineering International. 2016. Núm. 32. Pag. 519-533.

[2] Serra Parajes, J.; Crespo Márquez, A; and Sola Rosique, A. “Criticality analysis for preventive maintenance optimization purposes in gas network infrastructures,” Proc. Inst. Mech. Eng. Part O J. Risk Reliab., 2018.Ges

[3] De La Fuente, A.; González-Prida, V.; Guillén, A.; Crespo, A.; Sola, A.; Gómez, J.; Moreu, P. (2018). Strategic view of an Assets Health Index for making long-term decisions in different industries. Safety and Reliability – Safe Societies in a Changing World. Haugen et al. (Eds). © 2018 Taylor & Francis Group, London, ISBN 978-0-8153-8682-7. Pp 1151-1156

[4] Naderian, A., S. Cress, R. Piercy, F. Wang, and J. Service. 2008. “An Approach to Determine the Health Index of Power Transformers.” Conference Record of the 2008 IEEE International Symposium on Electrical Insulation (July 2008):192–96.

[5] UK DNO Common Network Asset Indices Methodology. (2017). Health and Criticality. Version 1.1. January 30th.

[6] De la Fuente, A; Candón, E; Martínez-Galán, P; Crespo, A; Sola, A and Moreu, P. (2018). Asset health index method for a process pumps fleet. Industria química, ISSN 2340-2113, Nº. 57, 2018 (Special ACHEMA 2018), Pp. 38-43

[7] ISO 14224, Petroleum, petrochemical and natural gas industries — Collection and exchange of reliability and maintenance data for equipment.

Evaluation of the power system reliability considering the renewable sources

Marko Čepin
Faculty of Electrical Engineering
University of Ljubljana,
Tržaška cesta 25, Ljubljana, Slovenia
marko.cepin@fe.uni-lj.si

Abstract

The tendency of the power systems develops in a direction that a larger number of smaller and intermittent power generating sources are introduced to the power system. The objective of the work is to investigate the related changes of the power system reliability due to the weather parameters, e.g. river flow which depends on precipitation. The selected method is the conventional loss of load expectation. In addition, its upgrade is developed, which is directed in sense that the actual possible power of the power plant is considered at specific time points instead of consideration of the nominal power at all time points. Such a method allows distinction between the power plants, which operate as necessary according to the load diagram, and the power plants, which operate as the environmental conditions allow. The results show that the power system reliability changes with the time according to the load diagram and according to the variable power capacity in time.

Keywords: power system, reliability, renewable sources.

1 Introduction

The power systems include more and more smaller and intermittent power generating sources. The large conventional thermal power plants and the large nuclear power plants face difficulties at the open market of electrical energy, where the subsidies for the renewable sources are exceeding the amount, which would not cause significant consequences on the open market of electrical energy. The consequence of huge amount of money invested in terms of subsidies for renewable power plants causes the decrease of the price of electrical energy, which causes the closure of the less competitive power plants, which are mostly coal thermal power plants. If their replacement by the wind power plants, the solar power plants and the other means of renewable power is considered, some prerequisites needs to be evaluated and assured. The energy balance needs to be assured, the power flow needs to be determined according to the load flow diagram, the frequency control needs to be assured and the appropriate power reserve needs to be secured in order that the quality of electric energy is not reduced. The power system reliability is hidden within definition of the electric energy quality, which requires acceptably constant frequency, acceptable shape of the voltage and the continuity of supply [1], [2], [3], [4], [5]. In other words, the interruptions are not desired for continuity of supply and this is measured through several indicators, which all somehow contribute to the power system reliability [6].

The objective of the work is to investigate the related changes of the power system reliability connected with the weather parameters (river flow as a consequence of precipitation, solar radiation and wind speed) through calculation of loss of load expectation. The focus is placed to the variability of hydro power, which can be later combined with the contribution of wind and solar power.

The selected method is loss of load expectation together with its upgrades [7]. The upgrades of the original method were performed in several ways [8], [11], [14], [15], [16], [17], [18], [19]. The recursive algorithm for consideration of a large number of power plants in the system was developed [5]. Namely, the number of states increases significantly $K=2^n$ with the number of power plants considered. So an advanced algorithm was developed, which can deal with the problem of large number of states. It is a recursive algorithm, which deals one plant at a time adding it to the model [5], [16]. In addition, attempts were made for ranking of the most important generating sources based on the reliability measures [1], [12].

2 Methods

The loss of load expectation (LOLE) is a method, which was developed for evaluation of the reserve in the power system in order to assure the required level of the static power system reliability. The method evaluates the expected time duration when the load is not being supplied with the required power capacity [7].

The probabilities of states of generating power plants are analysed in sense of the combinations where the generating power plants are considered one by one as available or unavailable with the respect to others [8], [9], [10]. The model of daily or monthly, or yearly load diagram is used to determine the number of hours of expected power production capacity shortages during the period considered, e.g. one day, one month or one year.

The mathematical model of the method is described in literature [5], [7], [11].

The basic equation representing the straightforward calculation of LOLE summarizes probabilities of state k, p(k), multiplied with the time durations of loss of capacity of state k, $t_{loss}(k)$, for the number of all states, K, where k is the index of specific considered state.

$$LOLE = \sum_{k=1}^{K} p(k) \cdot t_{loss}(k) \tag{1}$$

The probability of each specific state (k) is determined based on the probabilities of each particular generating power plant. The generating capacity can be available or not available. The number of all power plants is represented by the number n. The number of available ones in specific state is the number n_1 and the number of unavailable ones in specific state is n_2. The probability of each specific state k is the product of availabilities of the available power plants and unavailabilities of the unavailable plants. The parameter a(r) means the availability of plant r and the parameter 1-a(s) means unavailability of plant s, calculated as the complement of its availability.

$$p(k) = \prod_{r=1}^{n1} a(r) \cdot \prod_{s=1}^{n2} (1 - a(s)) \tag{2}$$

Forced outage rate, which is normally available for most of the plants, represents the unavailability of the plant.

Table 1 shows an example calculation of LOLE, where three power plants are considered. The nominal power of the first is 40 MW and it is 30 MW and 10 MW for the second and the third, respectively. Daily load diagram is represented by the curve and indicates the constant power of 55 MW in the first hour and 35 MW for the next 11 hours and 20 MW for the rest of the time, which represents the last 12 hours of one day.

For state 1 (k=1), all the units A, B and C are in operation, which means that the power system capacity in service equals to 80 MW. None of the plants is unavailable, thus the power capacity of power plants which do not operate is 0 MW, or the capacity lost is 0 MW. The probability of state 1 is the product of three specific plant availabilities (0.9·0.95·0.96=0.8208). The power of the capacity in service (80 MW) is larger than the load in the load diagram for all the time considered (24 hours), so the time duration of the loss of capacity where this would not be true, is $t_{loss} = 0$.

In state 2, the plants A and B are operable and the plant C is not operable. The power capacity of the power system is 70 MW. The power capacity lost is 10 MW, because the plant C with this power is the only one not available. The power of the capacity in service (70 MW) is larger than the load in the load diagram for all the time considered (24 hours), so the time duration of the loss of capacity where this would not be true, is $t_{loss} = 0$.

In such a way, all the rows of the capacity table are filled up.

In state 7, only the plant C is considered operable, so the power capacity in service is 10 MW. The capacity lost is 70 MW as this is the sum of power capacity of both power plants A and B, which do not operate. In this state, the load is all the time larger than 10 MW and the power capacity is insufficient for 24 hours, thus T_{loss} = 24 hours.

Table 1: Example calculation of LOLE

State	Unit A	Unit B	Unit C	Capacity lost	Capacity in service	Probability of each capacity state	p(k)	$t_{loss}(k)$ (h)	
k	40 MW	30 MW	10 MW	(MW)	(MW)				
	a(A)= =0.9	a(B)= =0.95	a(C)= =0.96						
1	1	1	1	0	80	0.9·0.95·0.96=0.8208	0.8208	0	0
2	1	1	0	10	70	0.90·0.95·0.04=0.0342	0.0342	0	0
3	1	0	1	30	50	0.90·0.05·0.96=0.0432	0.0432	1	0.0432
4	0	1	1	40	40	0.10·0.95·0.96=0.0912	0.0912	1	0.0912
5	1	0	0	40	40	0.90·0.05·0.04=0.0018	0.0018	1	0.0018
6	0	1	0	50	30	0.10·0.95·0.04=0.0038	0.0038	12	0.0456
7	0	0	1	70	10	0.10·0.05·0.96=0.0048	0.0048	24	0.1152
8	0	0	0	80	0	0.01·0.05·0.04=0.0002	0.0002	24	0.0048
							LOLE (hours/day)=		0.3018

Figure 1 shows the load diagram for the example calculation.

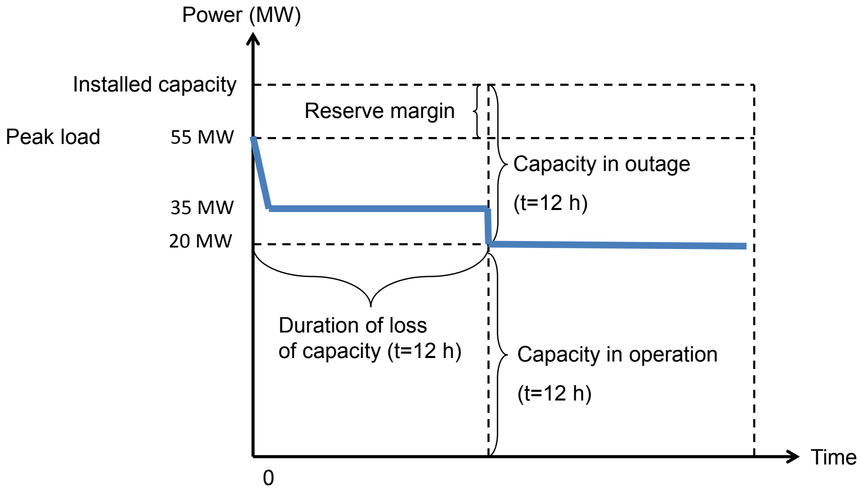


Figure 1: Example calculation of LOLE

The method was improved in sense that the static calculation of LOLE is made more dynamic by considering the actual power of the power plants, which power depends on the weather parameters, instead of the nominal power through all the time considered. In each time interval, the evaluation was performed by considering actual power of the power plants. The supporting computer code was developed, which can consider static LOLE or its upgraded evaluation, where in every hour (or an instance of an hour) the changes of the power generating capacities are considered. It allows consideration of the actual power changed in time instead of considering the nominal power as a constant. Figure 2 shows an example variability of the generating capacity variability in the selected power system, which can be considered by the developed computer code. The variability depends on the weather parameters, which mean variability of the river flow dependent on precipitation and other weather parameters.

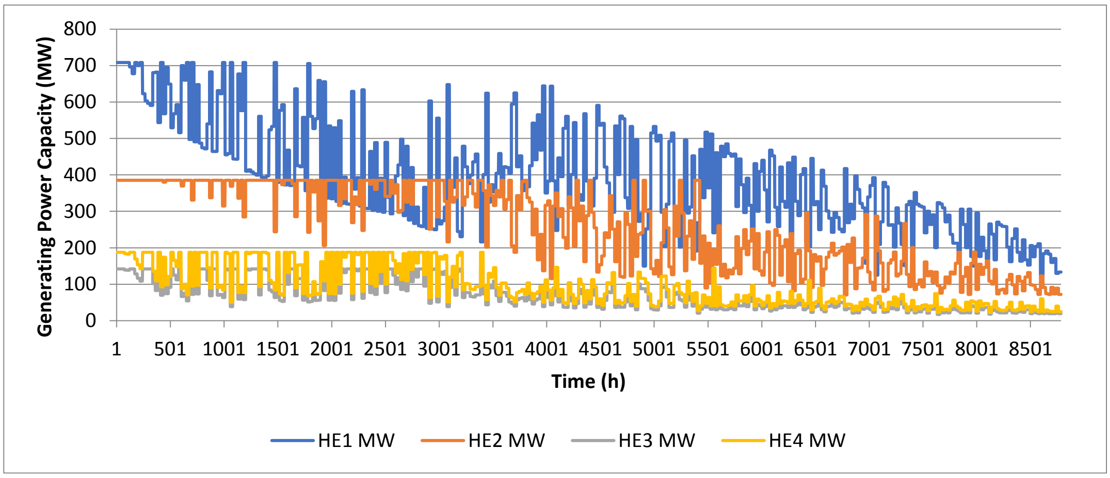


Figure 2: Example variability of generating capacity variability in the selected power system

3 Analysis and Results

Example includes power system with 77 power plants and suits the real regional power system. Table 2 shows a part of the plant data: plant identification, its nominal power and its forced outage rate (FOR). Figure 3 shows the load diagram, which is ordered by the load required by the power system and not by the running time.

Table 2: Example plant data (part of the complete table)

Plant Identification	Power (MW)	FOR	Plant Identification	Power (MW)	FOR	Plant Identification	Power (MW)	FOR
NEK	696	0.01	HEDEMOŽB1	24.4	0.01	HESELMAV2	19	0.01
TEŠ6	544	0.08	HEDEMOŽB2	24.4	0.01	HESELMED1	12.5	0.01
TEŠ5	316	0.09	HEDEMOŽB3	24.4	0.01	HESELMED2	12.5	0.01

Figure 4 shows the results. Loss of load expectation is calculated for every time point considering the real power plant power in the particular time point instead of the nominal power. Dotted line shows the average loss of load expectation, while the full line shows its values evaluated in all the time points. Normally, if the capacity of the power plants in the system is smaller, the loss of load expectation is larger and thus the power system reliability is smaller. The results show that the most of the time, the loss of load expectation is small enough. If its value is less than couple of hours per year, the reliability of the power system is sufficient. Namely, the reliability guidelines in some countries are determined considering the quantitative value of the loss of load expectation.

The results presented on figure are expected because the selected power system has a large reserve power. The peak load is 2660 MW and the theoretical power capacity of the system is 4818 MW.

With less reserve power, the loss of load expectation can increase significantly if some power capacity is not available.

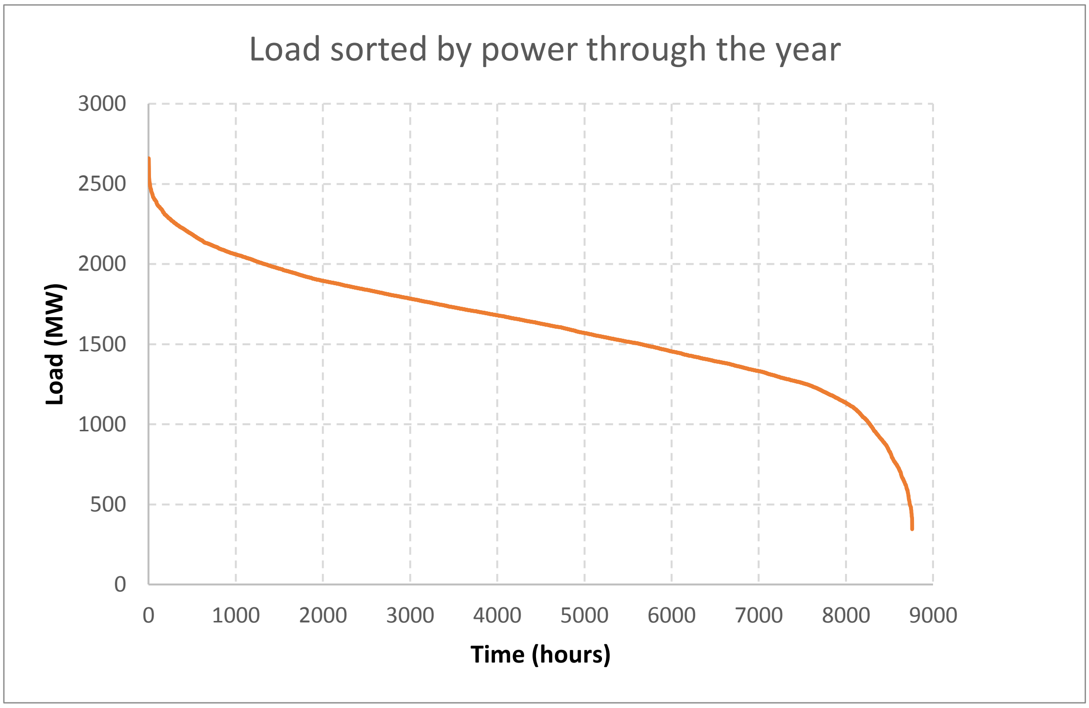


Figure 3: Load diagram for the selected power system

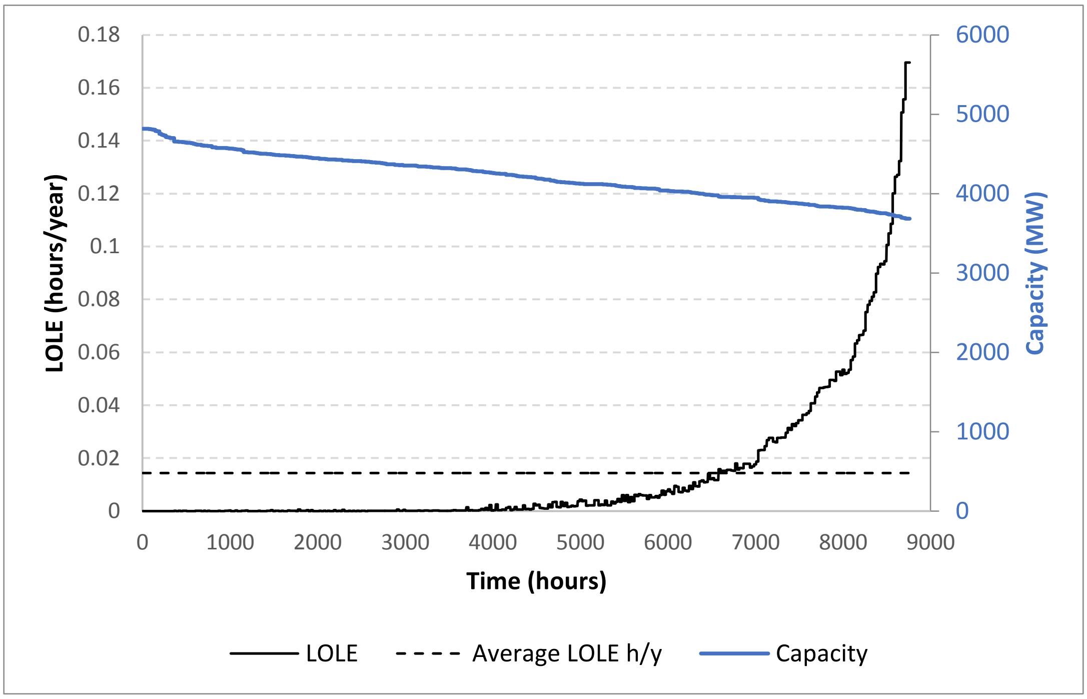


Figure 4: Calculated LOLE for the selected power system

Figure 5 shows the results of the similar power system with some plants less and with total capacity of the system 4120 MW. The peak load is the same as for the initial example system and it is 2660 MW. The calculated loss of load expectation is significantly higher and consequently the power system reliability is significantly lower. For a notable time of the year its reliability is even not within the guidelines (less than 2.4 hours per year for example guidelines, or less than 10 hours per year for other example guidelines).

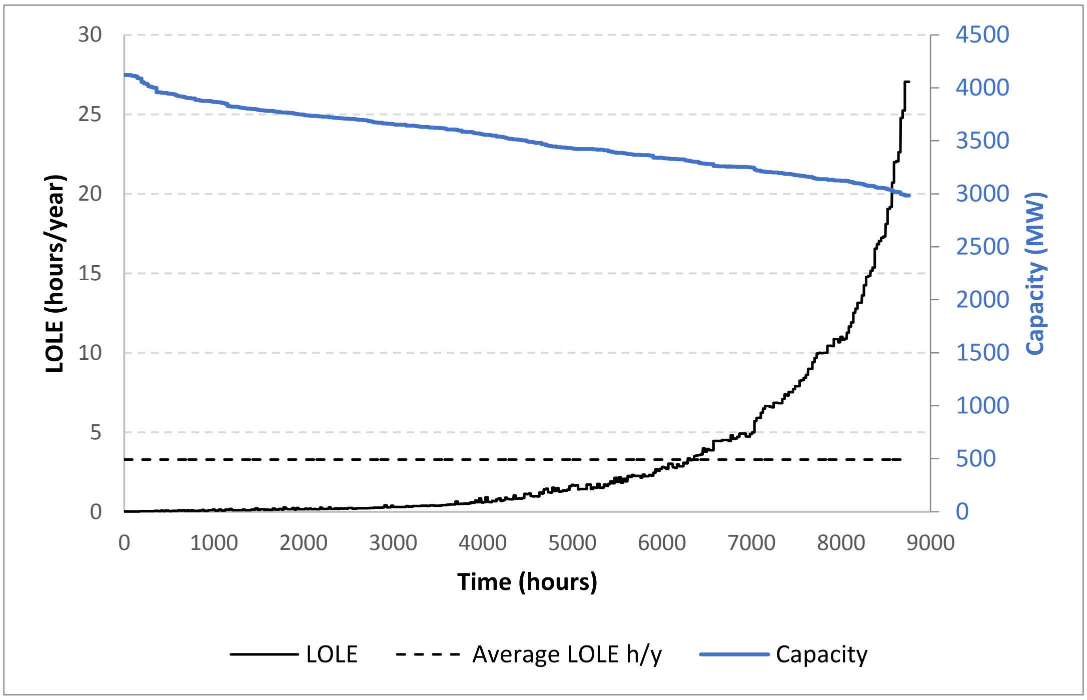


Figure 5: Calculated LOLE for the selected power system

If the conventional power plants are replaced with renewables, the average reserve power may decrease and the system reliability may decrease, which needs to be considered at the power system planning.

4 Conclusions

The objective of the work is to investigate the related changes of the power system reliability due to the weather parameters, e.g. river flow which depends on precipitation. The computer code was prepared to evaluate the upgraded loss of load expectation method, which facilitates the calculation of the load of load expectation for various time points, where the actual power of the power plants is considered in specific time intervals together with the yearly load diagram and together with the plant reliability data.

The example was selected as a case study and the data of the regional power system with 77 power plants was considered for evaluation. The results show good reliability of the power system, because the power reserve in this system is large. If the reserve is decreasing, the reliability can decrease significantly. This needs to be considered when the changes in the power system are made, specially, in the case of shutting down large power plants, which can operate all the time on nominal power and adding more intermittent power plants with theoretically large nominal power, which can be relatively difficult to be reached for a notable percentage of the year.

5 Acknowledgements

The Slovenian Research Agency partially supported this research within the research program P2-0356.

6 References

[1] Čepin M., Assessment of power system reliability, Springer, 2011.

[2] Anders G. J., Probability concepts in electric power systems, John Wiley and Sons, 1989.

[3] Billinton R., Allan R., Reliability evaluation of power systems, Plenum Press, 1996.

[4] Elmakias D., New computational methods in power system reliability, Springer Verlag Berlin Heidelberg, 2008.

[5] Wang X., McDonald J.R., Modern Power Systems, McGraw-Hill, 1994.

[6] IEEE Std 1366, Guide for electric power distribution reliability indices, IEEE, 2003.

[7] Calabrese G., Generating reserve capacity determined by the probability method, AIEE Trans, 1947, 66:1439-50.

[8] Garver L. L., Effective Load Carrying Capability of Generating Units, Transactions On Power Apparatus And Systems Vol 85, No 8, August 1966, p. 910 – 919.

[9] Čepin M. Evaluation of the power system reliability if a nuclear power plant is replaced with wind power plants, Reliability Engineering & System Safety, Vol. 185, 2019, p. 455-464.

[10] Bricman Rejc Ž., Čepin M., An improved method for power system generation reliability assessment (in Slovenian), Electrotechnical review, 2013, vol. 80, no. 1/2, p. 57-63.

[11] Bricman Rejc Ž., Čepin M., Estimating the additional operating reserve in power systems with installed renewable energy sources, International journal of electrical power & energy systems, 2014, vol. 62, str. 654-664.

[12] Čepin M., Volkanovski A., New importance factors in electric power systems (in Slovenian), Electrotechnical review, 2009, vol. 76, no. 4, p. 177-181.

[13] Mancarella P., Puschel S., Zhang L., Wang H., Brear M., Jones T., Jeppesen M., Batterham R., Evans R., Mareels I., Power System Security Assessment of the future National Electricity Market, University of Melbourne, 2017.

[14] Kirn B., Čepin M., Topič M., Effective load carrying capability of solar photovoltaic power plants - case study for Slovenia, Safety & reliability: theory and applications: Proceedings of the 27th European Safety and Reliability Conference, Taylor & Francis, 2017, p. 3231-3239.

[15] Čepin M., Reliability of power system considering replacement of conventional power plants with renewables, ESREL 2018, Safety and Reliability – Safe Societies in a Changing World – Haugen et al. (Eds), Taylor & Francis Group, 2018, p 63-70.

[16] Phoon H. Y., Generation System Reliability Evaluations with Intermittent Renewables, MSc. Thesis, University of Strathclyde, September 2006.

[17] Dehghan S., Kiani B., Kazemi A., Parizad A., Optimal Sizing of a Hybrid Wind/PV Plant Considering Reliability Indices, World Academy of Science, Engineering and Technology, Vol. 3, No. 8, 2009, p. 527-535.

[18] Abdullah M., Muttaqi K., Agalgaonkar A. P., Sutanto D., A noniterative method to estimate load carrying capability of generating units in a renewable energy rich power grid, IEEE Transactions on Sustainable Energy, vol. 5, (3) 2014, pp. 854-865.

[19] Wangdee W, Li W., Billinton R., Pertinent factors influencing an effective load carrying capability and its application to intermittent generation, International Journal of Systems Assurance Engineering and Management, Vol. 1 (2), 2010, p. 146–156.

Degradation Analysis and Preventive Maintenance Modelling and Assessment for Improved Resilience of Critical Infrastructures – Application to Torrent Checkdams

Chahrour Nour, Hariri Sleiman, Tacnet Jean-Marc
Univ. Grenoble Alpes, Irstea, ETNA, 38000 Grenoble, France.

Bérenguer Christophe
Univ. Grenoble Alpes, CNRS, Grenoble INP, GIPSA-lab, 38000 Grenoble, France.

Abstract

Natural threats have become more familiar, to the extent that requires ensuring the resilience of critical infrastructures. Critical infrastructures have always been complicated to study and assess, as they are all characterized by a collection of components that have numerous dependencies and interactions. Recently, several methods and frameworks have been put forward to assess and analyse comprehensively system's resilience. However, these methods have insufficiencies in identifying some hidden risks arising in a complex infrastructure. Therefore, it is essential to go beyond conventional methods and to develop risk strategies and decision-making techniques in order to overcome classical static assessment methods. This paper contributes to analyse the context of critical infrastructures with the ultimate objective of proposing new methods of choosing preventive maintenance strategies. It represents a modelling approach based on Petri nets to study the dynamic behaviour of the system when exposed to deterioration mechanisms and to support maintenance decision-making. The application is carried out on torrential checkdams in which the model results are presented and discussed in the paper.

Keywords: Critical infrastructures, degradation modelling, preventive maintenance, decision-making, Petri nets, checkdams.

1. Introduction

Recently, societies have become more and more reliant on infrastructures which constitute a network of man-made systems that delivers permanently and cooperatively major benefits, supplies, and services (e.g. electric power, telecommunication, transportation, water supply). Infrastructures are important for enhancing social environment and for economic prosperity. However, the complexity and interdependency of these infrastructures have turned them into a critical system-of-systems [1].

Critical infrastructures (CIs) are usually exposed to various types of threats (technical, natural, man-made attacks, etc.) which cause them damage. Consequently, the destruction or weakness of CIs may foster the risk due to the resulted impact on the economy, safety, and society as a whole [2]. Hence, analysing their reliability and safety but also choosing the best maintenance strategy is very essential. The internal or external interdependencies of CIs might also trigger risk such as the risk of cascading failures [3]. In other words, an initial failure of a CI which has dependencies with other CIs can result in disastrous proportions across the whole system. This reveals that interdependency increases the complexity of the system of CIs [4]. Nevertheless, not all infrastructures are considered to be critical. They can be classified based on a criticality scale which is identified after assessing the impact of the infrastructure disruption [5].

Another kind of CIs is linked to protection works against natural phenomena. Protection structures in the mountainous regions (e.g. Alpine) seek to fight against natural hazards generated in these areas. Torrents, avalanches, landslides, and other mountainous natural phenomenon are mostly caused by a gravitational and rapid movement of complex mixtures of fluids and solids [6]. According to the intensity of each natural phenomenon, several damages may arise. The impact can be expressed by the extent of the area that has been destructed, number of people affected, materials and assets disrupted (buildings, roads, infrastructures, etc.), financial damages, and the recovery rate of the resulted deterioration.

Due to the fact that torrential protection works (checkdams, sedimentation dams, levees, etc.) aim in preventing or mitigating the risk and thus protect people and assets from the imposed danger resulting from the natural phenomena, deep attention has been given to them. Unfortunately, protection works age, deteriorate, and may be damaged overtime when exposed to hazards. Their deterioration will influence their level of performance and thus will affect the possibility of reducing risk as much as it should be reduced. Moreover, these structures are interdependent in which a failure of a certain component (one structure) of the system (series of protection works) can lead to the perturbation of other components within the same system. Also, certain type of failure in one component may trigger another type of failure in the same component. All of the previous aspects lead to the conclusion that protection works are complex structures and can be considered as CIs. Checkdams are the most used torrential protection works in France. They represent around 14,000 civil engineering protection works in the French state forests [7].

To better understand the ability of protection structures in preventing damage, mitigating losses, and to be restored after an event requires mainly resilience analysis [8]. The term resilience refers to the ability of a system to withstand and adapt unfavourable events and its capacity to be recovered after being influenced due to such situations. Resilience analysis will give a comprehensive knowledge regarding the performance of these structures during and after the occurrence of hazards. Researchers have suggested several methods for quantifying resilience. Some researchers have concentrated on modeling the restoration of critical structures especially for bridge [9] and railway track [10] asset management hoping to improve their resilience.

Due to the fact that the system can be repaired following different maintenance strategies, decision-aiding models can help to choose the most preferable strategy.

These models analyse the behavior of the system over its lifetime period while being deteriorated or repaired. Such decision-aiding models can be implemented and assessed using Petri nets modeling tools and Monte Carlo simulation, which allow choosing between several maintenance strategies based on degraded-state conditions.

This paper is organised as follows: Section 2 introduces the methodology used to implement the desired model; Section 3 presents the modelling approach which models the behaviour of the system from one state to another; Section 4 considers a case study applied on check dams after identifying the possible failure modes and maintenance strategies; Finally, section 5 provides results coming from the simulation of the model.

2. Methodology Used: Stochastic Petri Nets (SPNs)

Petri nets (PNs) are dynamic models used in modelling the behaviour of a system (e.g. failure, repair, etc.) and in dependability calculations [11]. They present a graphical and mathematical tool for modelling complex systems and their evolution over time. Carl Adam Petri was the German who invented the graphics and the rules of PNs in the 1962 to be used in automation systems [12]. PNs allow analysing the dynamic behaviour of the system by modelling the transitions between its different states. Following their invention, PNs were developed by going far from traditional analytical approaches and using Monte Carlo simulation instead. In addition, the use of stochastic transitions has proven its efficiency for dependability (reliability, availability, and maintainability) analysis and for system safety [13].

Recently, SPNs are used to model complex systems, mainly the deterioration of critical infrastructures, such as railway networks [14]. SPNs are particularly well suited to model the evolution of the system while changing from one state to another and are able to compute the time spent by the system in each state and the number of each type of intervention that was carried out based on Monte Carlo simulation [15]. They can therefore extend and complement existing methods providing static effectiveness assessment [16].

PNs are a collection of four main elements. Places represent a condition and reflect the state of the system and are symbolized by circles. Transitions are symbolized by rectangles and correspond to events that cause a change of state in the system. The state of the system is characterized by marking places with tokens. Arcs are arrows that connect a place to a transition or a transition to a place only. They are associated with multiplicities which are responsible for the operation of the PN. If an arc does not indicate any multiplicity, the value will be one by default.

Once the PN model is constructed and the lifetime period t_f of the system is identified, Monte-Carlo simulation starts and the tokens will keep on moving around the model until t_f is reached. The movement of tokens is governed by the following rules:

1. When the number of tokens in each input place of a transition is at least equal to the multiplicity of the arcs connecting each, the transition is enabled and will be fired after a specified transition firing time.
2. When a transition is fired, a number of tokens equal to the multiplicity of the arc is removed from the input places, and added to the output places.

An additional characteristic of PNs is the inhibitor arc. This arc is represented by a dotted arrow and can be only directed from a place to a transition. Its aim is to inhibit the firing of the transition which it is connected to when its multiplicity is equal to the number of tokens located in its input place.

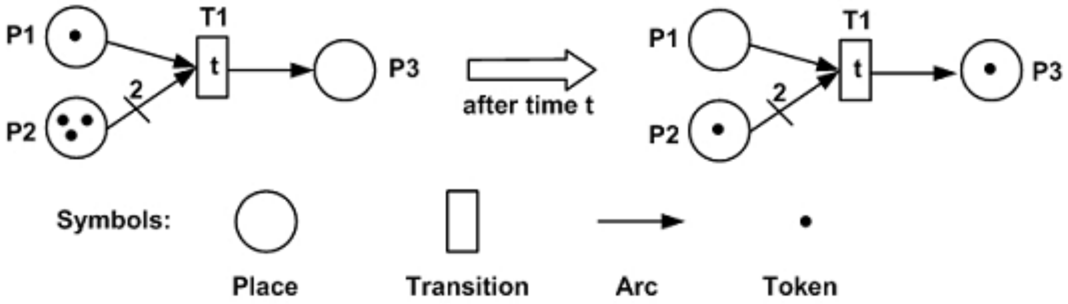


Figure 1: Simple PN showing the transition firing process.

A simple PN is illustrated in Figure 1. P1 and P2 are both marked with a number of tokens satisfying the rule of enabling a transition. Therefore, T1 is enabled. After time t, T1 is fired in which 1 token (multiplicity = 1) is removed from P1, 2 tokens (multiplicity = 2) is removed from P2, and 1 token (multiplicity = 1) is added to the output place P3.

3. SPN Modelling and Assessment Framework for a Deteriorating Structure

In this section, a general modelling framework using SPN is presented. The aim is to represent the evolution of the state of a CI when exposed to degradation mechanisms or to maintenance operations and then to support decision-making by comparing different maintenance strategies.

3.1 Degradation, inspection, and maintenance processes

The modelling of the degradation process is illustrated in Figure 2 [17]. P1-P4 represents the four degraded states which are linked by stochastic transitions T1-T3 associated with exponential distribution firing times assumed and judged by an expert. In order to detect the state of the system, inspection must be carried out periodically. At t=0, a token is added to P1 (initial state) and to P5 waiting for T5 to fire so that the token moves to P6 where inspection takes place. In this study, inspection is scheduled every year. After the firing of one of the immediate transitions T6-T8, the condition of the system is revealed where a token appears in one of the places P7-P9. In this case, the respective maintenance operation begins and after a specific time needed for reparation, T9, T10, or T11 fires depending on the condition revealed and the system returns back to its initial state waiting for another inspection.

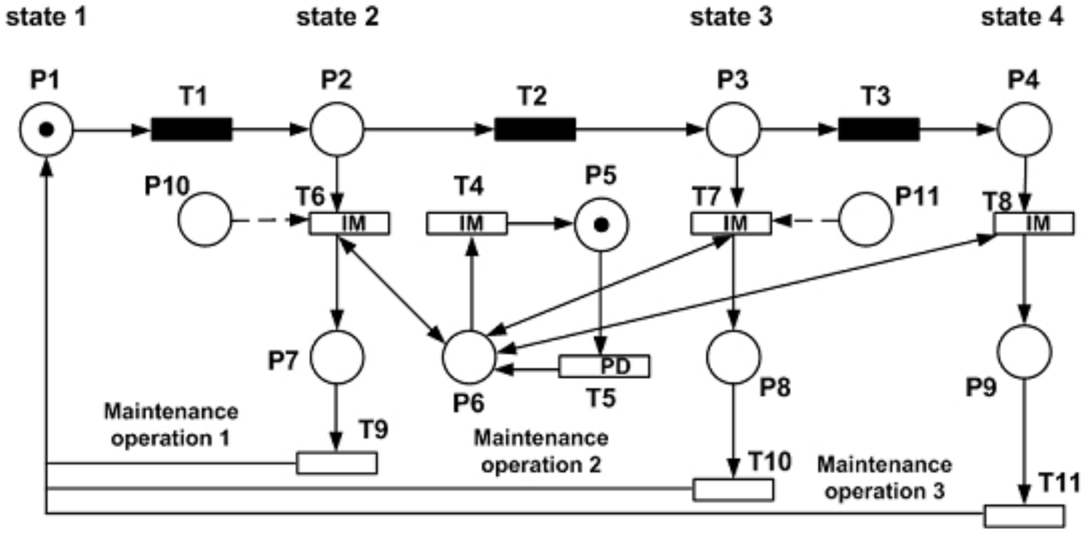


Figure 2. A basic PN model showing the degradation, inspection, and maintenance processes [17].

3.2 Decision-making support

In order to make a decision and choose between the different possible maintenance operations, inhibitor arcs should be added to the model. The presence of a token in P10 or in P11 inhibits respectively maintenance operation 1 or maintenance operation 2 from being carried out over the lifetime period of the system.

After implementing each strategy, the results provided after Monte Carlo simulation reveals the time spent by the system in each state (sojourn time) and the number of maintenance operations performed within the lifetime period of the system. These outputs allow comparing between the different maintenance strategies in terms of time and cost.

4. Application to Checkdams

Checkdams, like any other protection structures, are constructed to perform certain functions. Their major functions involve bed stabilization, bed elevation and slope reduction, retention of sediment deposits, flow centring, and prevention of longitudinal erosion. However, due to their age, wear and tear, and the intensity of the phenomenon that they must resist, different kinds of pathologies may appear affecting their performance level. The assessment of the efficacy of protection structures to reduce risk is based on three components: structural, functional, and economical efficacy [16]. To limit their degradation, these structures should be inspected and maintained regularly. Besides, in order to choose a suitable maintenance strategy, it is important to have a comprehensive knowledge on the types of failures that checkdams may be subjected to.

It is also essential to differentiate between functional and structural failures. This is due to the fact that the structure may be stable from a structural point of view but is not fulfilling a certain function. On the other hand, the structure may have some bad structural properties but is still fulfilling its functions. Structural failures are linked to the external (e.g. sliding, overturning, etc.) and internal (e.g. reinforcement, material strength, etc.) stability of the structure. Functional failures includes the phenomena of lateral bypass in which the dam is no more able to release the flow from its hydraulic section and the phenomena of scouring where intense clear water flow removes the soil under the base of the dam's foundation.

The present study aims to prove the ability of SPN models in choosing between different maintenance strategies to be applied on checkdams highlighting on some aspects such as time, cost, and efficiency. The application presented below aims to study the stability of a checkdam when exposed to scouring. Figure 3, represents the different possible functional (FS) and structural (SS) states of the dam depending on the increase level of scouring under the foundation.

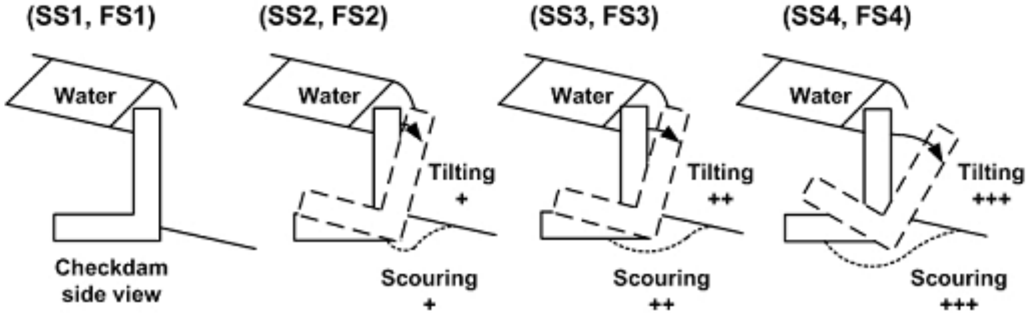


Figure 3. State-degradation due to scouring under the foundation of a checkdam.

In this paper, the functional and structural degradations are modelled separately without taking into account the dependencies and interactions between both failures.

4.1 Evaluation of functional degradation states

In this section, the SPN model describes the behaviour of the checkdam when exposed to functional failure. The different functional states are presented assuming that the system is stable from a structural point of view. Four stability states were defined as shown in Figure 4. Regarding maintenance operations: minor maintenance can be applied when the slight deterioration can be easily repaired (SS1, FS2), major maintenance is needed in order to repair the serious degradation level that the structure has reached (SS1, FS3), and corrective maintenance is required when the structure completely fails and should be replaced (SS1, FS4).

Thus the structural state is fixed to SS1 and four functional states are defined FS1, FS2, FS3, and FS4 corresponding to an increased level in scouring. When the system is not in its initial state, minor, major, or corrective (replacement) maintenance operations are to be carried out.

In addition, the system can only be maintained by three minor operations and two major operations before replacing the system with a new one. This is illustrated by the presence of P12 and P13 (Figure 4) linked with inhibitor arcs with respective multiplicities 3 and 2. Meaning that when 3 tokens appear in P12, minor operations are inhibited and when 2 tokens appear in P13, major operations are inhibited. However, after each replacement, P12 and P13 should be emptied from tokens in order to enable again minor and major operations. This function is included within the properties of T11 (reset transition) in which upon firing, it removes all the tokens in P12 and P13.

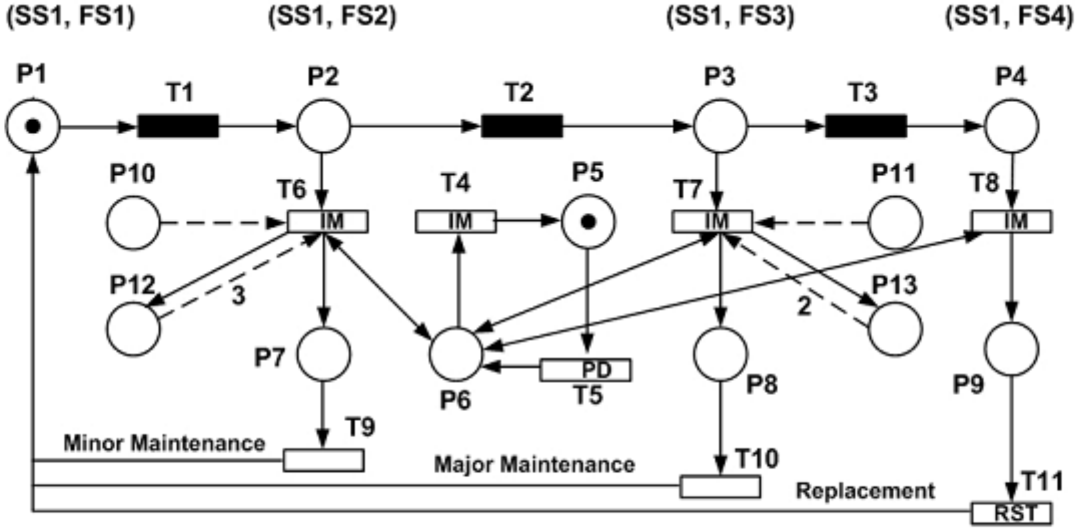


Figure 4. SPN model showing the functional degradation, inspection, and maintenance processes (improved and adapted version of [17]).

The input data needed to run this model are the firing delay times associated with each transition. In this study, no historical data are available, therefore these data are assumed and assessed by experts in the field of checkdams and presented in Table I and Table II.

Four different strategies are identified. In strategy 1, reparation is done as soon as the condition revealed after inspection does not correspond to the new state. In strategy 2, a token is added to P10 which inhibits minor operations. In strategy 3, a token is added to P11, thus major operations are inhibited. In strategy 4, P10 and P11 are marked with tokens meaning that only corrective maintenance can be carried out.

Table I: Failure rates of degraded-states transitions.

Transition	Exponential Failure rate λ (years^{-1})
T1	0.5
T2	0.1
T3	0.033

Table II: Constant transitions firing times.

Transition	Firing time (years)
T4 T6 T7 T8	0
T5	1
T9	0.013
T10	0.022
T11	0.041

4.1 Evaluation of structural degradation states

In this section, the SPN model describes the behaviour of the checkdam when exposed to structural failure. The different structural states are presented assuming that the system is fixed to a functional state FS3 where scouring already exists. Four structural states are defined SS1, SS2, SS3, and SS4. The structural state of the dam degrades in which the dam will start to tilt until it finally overturns when scouring reaches a critical level. Scouring level can be used as an indicator to describe the behaviour of the checkdam from structural point of view. The four different stability states are represented in Figure 5.

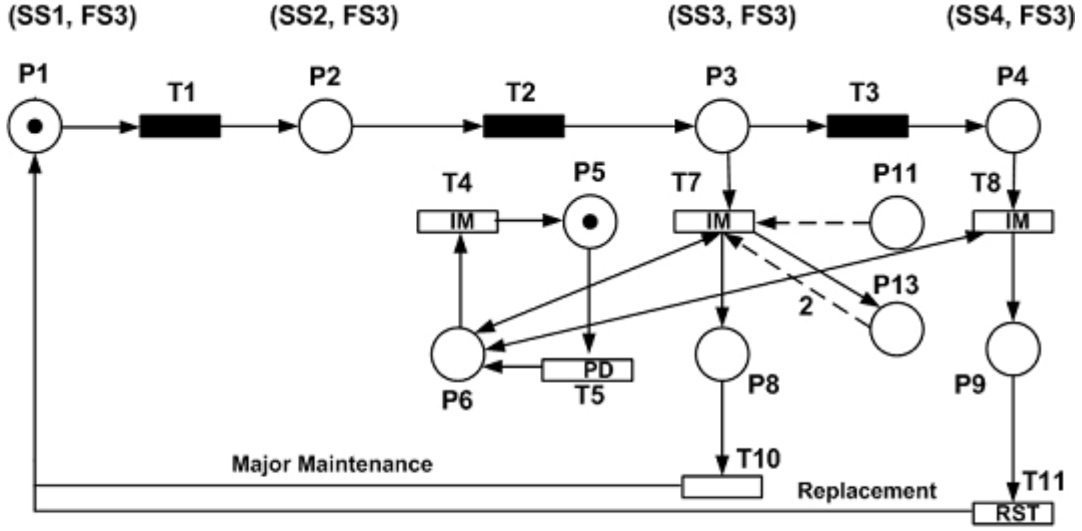


Figure 5. SPN model showing the structural degradation, inspection, and maintenance processes (improved and adapted version of [17]).

Regarding maintenance operations: major maintenance can be applied by reinforcing the checkdam to avoid its failure by overturning after reaching state (SS3, FS3) and corrective maintenance is required when the structure completely fails and should be replaced (SS4, FS3). In state (SS2, FS3), the checkdam is subjected to mild tilting in which no need for a maintenance operation to be carried out at this stage. Moreover, Figure 5 reveals that only two major operations can be carried out before the replacement of the system. The firing delay times corresponding to structural deterioration are estimated by an expert and given in Table III and Table IV.

Table III: Failure rates of degraded-states transitions.

Transition	Exponential Failure rate λ (years^{-1})
T1	0.5
T2	0.25
T3	0.5

Table IV: Constant transitions firing times.

Transition	Firing time (years)
T4 T7 T8	0
T5	1
T10	0.082
T11	0.33

For structural degradation, two maintenance strategies are suggested. In strategy 1, reparation is done when the system reaches state (SS3, FS3). In strategy 2, P11 is marked with a token in which only corrective maintenance can be carried out.

5. Results

The SPN models are constructed using GRIF-Workshop developed by TOTAL. The simulation of the previous models is based on Monte-Carlo simulation. After each simulation, the mean sojourn time in each state and the number of maintenance operations carried out during the lifetime period of the system will be given. The model is simulated over a period of 100 years. It is noticed that convergence in results occurs after 200 simulations. Tables V - VIII provide all the results obtained after the simulation of the different strategies applied for functional and structural degradation over a period of 100 years.

Table VI reveals the effect of each maintenance strategy on the mean sojourn time. It is noticed that the longest sojourn time in the initial state (21 years) occurs by performing strategy 1. This is due to the fact that the system is repaired as soon as it degrades further from the initial state. For strategy 2, minor operations are inhibited, thus the system will remain in a degraded state for a long time. This is the reason behind the decrease in the sojourn time in the initial state (11 years) when applying strategy 2.

Table V: Average expected number of interventions - functional degradation.

Strategy	Minor Maintenance	Major Maintenance	Corrective Maintenance
1	6	3	1
2	0	4	1
3	7	0	2
4	0	0	3

Table VI: Average expected sojourn time (years) – functional degradation.

Strategy	(SS1, FS1)	(SS1, FS2)	(SS1, FS3)	(SS1, FS4)
1	21	46	32	0
2	11	53	35	1
3	20	24	55	1
4	6	28	65	1

Table VII: Average expected number of interventions – structural degradation.

Strategy	Major Maintenance	Corrective Maintenance
1	8	5
2	0	11

Table VIII: Average expected sojourn time (years) – structural degradation.

Strategy	(SS1, FS3)	(SS2, FS3)	(SS3, FS3)	(SS4, FS3)
1	30	56	11	2
2	25	46	22	6

In Table VIII, it is also clear that when major maintenance is inhibited, the sojourn time of the system in the initial state (SS1, FS3) will be less than that when maintenance is applied directly if the system degrades to state (SS3, FS3). The results obtained in Table V and Table VII, allow comparing the different strategies in terms of cost. It is assumed that for functional degradation, the cost of minor maintenance, major maintenance and corrective maintenance are 5 000 €, 15 000 €, and 45 000 € respectively. For structural degradation, it is assumed that the cost of major maintenance and corrective maintenance are 60 000 € and 150 000 € respectively.

Knowing the cost of each type of operation and using the data in Table V and Table VII, the total cost of each strategy can be computed. The results are given in Table IX and Table X. It can be seen that for functional degradation, strategy 4 is the most expensive because of the huge number of corrective maintenance to be done (3 replacements). Strategy 2 has the lowest cost since the system is allowed to deteriorate before being maintained with minor operations.

Table IX: Total maintenance cost (€) for each strategy – functional degradation.

Strategy	Minor Maintenance	Major Maintenance	Corrective Maintenance	Total Cost
1	30 000	45 000	45 000	120 000
2	0	60 000	45 000	105 000
3	35 000	0	90 000	125 000
4	0	0	135 000	135 000

Table X: Total maintenance cost (€) for each strategy – structural degradation.

Strategy	Major Maintenance	Corrective Maintenance	Total Cost
1	480 000	750 000	1 230 000
2	0	1 650 000	1 650 000

Similarly, for structural degradation, strategy 2 is more expensive than strategy 1 due to the large number of corrective maintenance operations.

6. Conclusion

This paper addresses the development of a decision-aiding method regarding resilience and maintenance of CIs. The main objective is to go beyond traditional safety and reliability techniques for efficacy and resilience assessment. Based on the results, SPN approach, combining Monte Carlo simulation and state-based modelling technique has proved to be favourable and can be an appropriate tool to be used later for 1) analysing the interdependencies among CIs and 2) choosing the best operating strategies. The limitations in this study include modelling the system without taking into account the dynamic interactions between the different failure modes that may occur on the structure and how an event may foster the occurrence of another event (accident sequence). Calculations are based on expert assumptions and further works are needed to improve and determine modelling hypothesis (e.g. failure rates). Furthermore, acquiring reliable results in the domain of resilience and preventive maintenance is not easy due to a number of barriers such as information imperfection and the absence of real historical data. This study will be developed by taking into consideration interdependencies which increase the risk of failure. The strong reliance on CIs points out that it is a priority to assure their safety and availability.

Acknowledgements

This work is supported by the French National Research Agency in the framework of the Investissements d’Avenir program (ANR-15-IDEX- 02).

References

[1] Eusgeld, I., Kröger, W., Sansavini, G., Schlöpfer, M., and Zio, E. (2009). The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. *Reliability Engineering and System Safety*, 94(5):954–963.

[2] Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering and System Safety*, 93(12):1781–1787.

[3] Duenas-Osorio, L. and Vemuru, S. M. (2009). Cascading failures in complex infrastructure systems. *Structural Safety*, 31(2):157 – 167.

[4] Rinaldi, S., Peerenboom, J., and Kelly, T. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6):11–25.

[5] Clarke, J., Coaffee, J., Rowlands, R., and Finger, J. (2015). Resilience evaluation and SOTA summary report. Technical report, Realising European ReSILiencE for Critical INfraStructure.

[6] Tacnet, J.-M. (2009). Prise en compte de l'incertitude dans l'expertise des risques naturels en montagne par analyse multicritères et fusion d'information. *PhD thesis, Ecole Nationale Supérieure des Mines de Saint-Etienne, France*.

[7] DI Ciocco, G. (2015). Conception et réalisation d'un environnement d'évaluation de l'efficacite fonctionnelle et structurelle d'ouvrages de protection contre les risques torrentiels. *Master's thesis, Polytech' Clermont Ferrand, France.*

[8] Ouyang, M., Duenas-Osorio, L., and Min, X. (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Structural Safety,* vol. 36, pp. 23–31.

[9] Le, B. & J. Andrews (2016). Petri net modelling of bridge asset management using maintenance-related state conditions. *Structure and Infrastructure Engineering* 12(6), 730–751.

[10] Andrews, J. (2013). A modelling approach to railway track asset management. Proceedings of the Institution of Mechanical Engineers, Part F: *Journal of Rail and Rapid Transit* 227(1), 56–73.

[11] Aubry, J.-F., N. Brinzei, and M. H. Mazouni (2016). *Systems Dependability Assessment: Benefits of Petri Net Models*, Volume 1 of Systems and Industrial Engineering Series. Systems Dependability Assessment Set. ISTE Ltd and John Wiley & Sons Inc.

[12] Petri, C. A. (1962). *Kommunikation mit Automaten*. Ph.D. Thesis, Mathematisches Institut der Universitat Bonn.

[13] Signoret, J.-p. (2009). Dependability & safety modeling and calculation: Petri nets. *IFAC Proceedings Volumes* 45(5), 203 – 208. 2nd IFAC Workshop on Dependable Control of Discrete Systems.

[14] Gaied, M., Lefebvre, D., M'halla, A., and Othmen, K. B. (2018). Modelling and Performance Evaluation of Railway transport Systems using P-timed Petri Nets. *5th International Conference on Control, Decision and Information Technologies (CoDIT)*, pp. 841-846.

[15] Zio, E. (2013, January). *The Monte Carlo Simulation Method for System Reliability and Risk Analysis*. Springer. ISBN 978-1-4471-4588-2.

[16] Carladous, S. (2017). Approche intégrée d'aide à la décision basée sur la propagation de l'imperfection de l'information-application à l'efficacité des mesures de protection torrentielle. *Ph.D . Thesis, Ecole des Mines de Saint-Etienne, France.*

[17] Hariri, S. (2018). Contribution to the evaluation of the reliability of interacting systems – application to checkdams maintenance strategies. *Master's thesis, Grenoble INP, France.*

Modelling resilience of complex engineered systems using service continuity approach

Lech A. Bukowski
WSB University
Str. Cieplaka 1c
41-300 Dąbrowa Górnicza, Poland

Abstract

The aim of this paper is to present the concept of the complex engineered systems resilience assessment in the case of disruptive events occurrence. Firstly, the basics of service dominant approach will be discussed, and then the concept of operationality related attributes of engineered systems will be presented. Finally, the structure of a general dependability model has been proposed, which consists of four partial models, namely: availability, safety, security, and resilience ones. On this basis, using the service continuity oriented approach, the quantitative model of complex engineered systems resilience will be proposed. For quantitative evaluation of the complex systems resilience to a disruption risk we propose the resilience metric - a collective term described by four main indicators: absorbability, recoverability, adaptability and disruptive event impact.

Keywords: resilience, modelling, service engineering, continuity, complex systems

1. Introduction

Traditionally the term resilience means the tendency or ability to spring back, and thus the ability of a body to recover its normal size and shape after being pushed or pulled out of shape, and general any ability to recover to normality after a disturbance. It means being able to withstand shocks and deviations from the intended state and go back to a desirable or acceptable state. *The function of a complex engineered system* is to generate results in line with the goals and objectives of the system, regardless of the state of the system and its environment. In practice, the function of *production systems* is the effective and efficient production of certain products, whereas *service systems* come down to providing services in accordance with the requirements of the customers at prices favourable to both sides. Therefore, *resilience for complex engineered systems* can be generally defined as *the ability to deliver, maintain and improve service when facing threats and evolutionary changes*.

A limitation of maximum tolerable disturbance measures is that we may well be interested in characterizing how well a system under consideration rebounds from smaller disturbances. For instance, given a form of fault tolerance that allows for some degradation of service, we may then want to measure not only how far the system can be pushed before failing altogether, but also the relationship between the size of disturbances and the degradation of performance. Since for most systems of interest the resilient behaviour is non-deterministic in practice, we are no longer interested in whether the system will rebound from a disturbance but in the probability of it successfully rebounding (survive) and the distribution of the time needed for the system to return to a desired state (recover). Thus in the area of dependable computing we talk about the 'coverage' factor of a fault-tolerant mechanism, and we can talk about the distribution of the latency (time to detection) of a component fault or data error (Avisienis et al. 2004).

A concern in the *resilience engineering* literature is that measures of outcomes may lack predictive power: success in the past is no guarantee of success in the future. Thus, a search for leading indicators that can be used to assess future resilience is difficult because of the multidimensionality of resilience. Westrum (2006) writes: "Resilience is a family of related ideas, not a single thing. The various situations that we have sketched offer different levels of challenge, and may well be met by different organizational mechanisms. A resilient organization under Situation I will not necessarily be resilient under Situation II (these situations are defined as having different degrees of predictability). Similarly, because an organization is good at recovery, this does not mean that the organization is good at foresight".

Although the ideas of vulnerability and resilience have been introduced relatively recently, they have already been examined in many serious studies, both theoretical and practical, in the area of engineered systems (e.g.: Aven 2011; Dekker et al. 2008; Holling et al. 2006; Kröger and Zio 2011; Francis and Bekera 2014; Park et al. 2013; Sheffi 2007) . Also in the area of service engineering and logistics a significant number of interesting works have been published (e.g.: Christopher and Peck 2004; Pettit et al. 2013; Peck 2006; Waters 2007). However, engineered systems as well as production and service processes within these systems are closely related to the human factor, the environment and cybernetic systems. Increasingly interconnected social, technical and economic networks create large complex engineered systems in a globalized society, and resilience assessment of many individual subsystems becomes more and more complicated, or even impossible. Thus, there is an urgent need for a comprehensive and holistic approach to the problem of ensuring resilience of complex engineered systems. This approach requires crossing the boundaries of particular disciplines, and therefore the application of *transdisciplinary perspectives*.

The objective of this paper is to develop a general resilience model for complex engineered systems which is based on the service continuity oriented approach. For this purpose, a review of the literature from the *service engineering perspective* was carried out, and on this basis the concept of *service continuity approach* was developed to perform quantitative evaluation of the vulnerability and resilience of complex engineered systems to a disruption risk.

2. Fundamentals of service dominant approach

A *service* can be described as: all intangible effects resulting from a client interaction that creates and captures value (ERISS, 2016). Currently, services combine both products and services, and the distinction between the two is fuzzy and vague. Services are offered by a provider to its consumers. Baida et al. (2004) defined business services as activities delivered by a service provider to a service consumer to create a value for the consumer. Business services are typically discovered and invoked manually, but their realization may be performed by automated or manual means. Services lack of concrete characteristics. Thus, services must be defined indirectly in terms of the effects they have on consumers. This makes the description of services one of the most important undertakings for the future.

*Service knowledg*e is an area of expertise which involves: business, management, industrial engineering, information and communication technology (ICT), socio-legal sciences, and economics. *Service science* has developed in response to the need to combine technological and non-technological innovations in a rapidly growing and changing environment. The discipline focuses on the innovative creation of value by using various transdisciplinary approaches. A service-dominant approach is starting to take over from the traditional goods-dominant approach. Main key factors of the *service-dominant approach* include:

- the realization of a service as a process,
- a focus on dynamic resources,
- outsourcing and globalization,
- complex interdependences between elements.

Service science, management, and engineering (SSME) is a term introduced by IBM to describe service science, an interdisciplinary approach to the study, design, and implementation of service complex systems in which specific arrangements of people and technologies take actions that provide value for others. SSME has been defined as the application of science, management, and engineering disciplines to tasks that one organization beneficially performs for and with another (Sampson 2010). *A Service System* is a term that frequently appears in the service management, service operations, services marketing, service design, and service engineering literatures (Salvendy and Karwowski 2010). Service involves both a provider and a client working together to create value. These relationships and dependencies can be viewed as a complex system in which the parts interact with each other in a non-linear manner, and which have emergent properties. In many cases, the main source of complexity in a service system is its people: the client, the provider, or other organizations.

Service engineering is a new methodology to the analysis, design and implementation of service-based ecosystems in which organizations and IT provide value for others in the form of services. Service Engineering not only provides methodologies to handle the increased complexity of numerous business actors and their value exchanges, but also provides tools for constructing and deploying services that merge the IT and business perspectives (Cardoso et al. 2009). Service Engineering is a structured approach for describing a part of an organization from a service perspective that expresses the way the organization works (Salvendy and Karwowski 2010). It provides a discipline for using models and techniques to guide the understanding, structure, design, implementation, deployment, documentation, operation, maintenance and modification of typical services as well as e-services. This approach should systematically translate an initial description from a natural language that expresses the way stakeholders think and communicate about the organization through a sequence of representations using various models to a representation that is accepted and understood by all the participants of the system.

The fast-growing discipline of service engineering is related to service economy growth and the global need for innovation, developing and implementing of different kinds of services (Sampson 2010). Often the biggest problem lies in bridging the gap between business and IT. This challenge requires a set of design principles, patterns, and techniques that currently have not been identified precisely enough. Therefore, the *Internet of Services* cannot be realized without giving a strong emphasis on both the business as well as the technological side of services.

The Unified Service Theory (UST) developed by Scott E. Sampson could serve as theoretical background for building the general model of Service Engineering. The basis for a UST is the assumption that*: "Services are production processes wherein each customer supplies one or more input components for that customer's unit of production"* (Sampson 2010). The concept of a process is defined in standards (e.g. EN ISO 9000:2015 and EN ISO 9001:2015) and in professional literature in a variety of ways. On the basis of considerations made in previous sections, it is proposed to adopt two types of process definitions. The first one was based on the systems theory ST system definition. It is of formal nature and reads as follows: *A process is a system whose elements are events and activities connected by flow relations.*

Events are a change in the state of the system or its environment which can initiate the start of a process, interfere with it causing errors and pauses or end it when the desired outcome is achieved. *Activities* are understood as intentionally designed and implemented actions. We divide them into:

- *Operations*, which apply to individual activities,
- *Tasks*, understood as sequences of activities or operations performed by the same 'actor' on the same object, and
- *Decisions*, which are choices, as a result of which the process can branch into two or more paths.

Flows are relations that consist in the movement of goods (transport) and information (communication). The process structure can be described in the form of a *PS* graph as following (Bukowski 2019):

$$PS \subset (E, A, R) \tag{1}$$

where: E - process initiating, disturbing and terminating events,
A – activities (operations, tasks, decisions),
R - relations between events and flow relations.

The components of the structure can be set up in the following form:

$$E = (e_i : i = 1, 2, 3, \dots, l) \tag{2}$$

$$A = (a_j : j = 1, 2, 3, \dots, m) \tag{3}$$

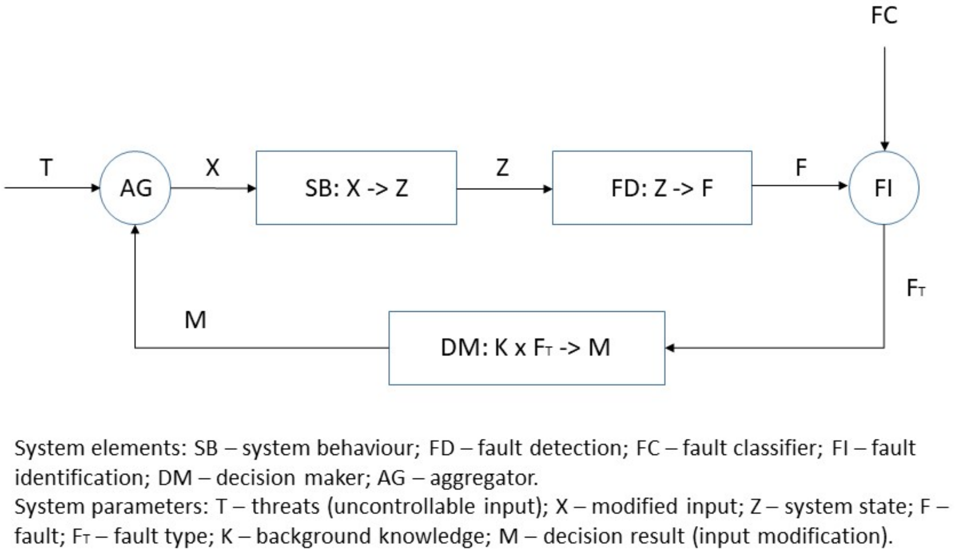
$$R = (r_k : k = 1, 2, 3, \dots, n) \tag{4}$$

Business practice recommends using descriptive definitions, therefore the following definition of a process is proposed: *A process is a structured chain of events and actions interconnected by flow relations, the aim of which is to achieve the desired result.*

Process approach is to be understood as the identification of processes, their dependencies and order, determination of the criteria and methods ensuring and evaluating effectiveness, regular monitoring, measurement and analysis, as well as the implementation of any corrective actions necessary to achieve planned results and their continual improvement.

3. Operationality related attributes of engineered systems

Based on the service dominant approach as well as the assumptions made in sections 1 and 2, we propose a general model of an engineered system - S, which is controlled for operationality reasons. The term *operationality* means *the ability of a given system to perform the required functions*.



System elements: SB – system behaviour; FD – fault detection; FC – fault classifier; FI – fault identification; DM – decision maker; AG – aggregator.
System parameters: T – threats (uncontrollable input); X – modified input; Z – system state; F – fault; F$_T$ – fault type; K – background knowledge; M – decision result (input modification).

Figure 1. General model of an engineered system with the operationality control (Bukowski 2019)

Figure 1 shows schematically the concept of this model, which is based on the control engineering rules. The main block of the system is a SB-element whose role is to transform the input X into the state of system Z. The next FD-block is responsible for the fault detection of the S system, assigning the appropriate faulty state kind F_i for each faulty Z_i state. The next step is FI – fault identification, in which the F_i is compared with the typical faults kinds given by the fault classifier FC. The result of the comparison in the form of a fault category F_C is supplied to the decision-maker DM, who based on his background knowledge K, makes decision M, which should modify the external input T so that the modified internal input X gives, after the transformation, the correct output Z (proper state of the system S).

In practice the correct service is delivered when the system's behaviour allows it to fulfil the required functions, described by the system specification. *A fault* is that part of the system states that may cause a subsequent failure. *A failure* is an event that occurs when a fault alters the service quality, and the delivered service deviates from a correct service. A system may fail either because it does not comply with the specification, or because the specification did not adequately describe its function. Thus, a failure is a transition from correct service to incorrect service, which means that the system does not implement the intended function. A transition from incorrect service to correct service is a service *recovery*. The time interval during which incorrect service is delivered is a *service outage*. A system can fail in different ways, therefore we can distinguish different fault categories and failure modes.

The ability to provide a service that can justifiably be trusted is called *dependability*, and is used as *a collective term describing the time-related operating quality of a system*. The concept of dependability includes the constituent properties that can be represented in the form of a "dependability tree", consisting of three levels. Dependability is divided into four main attributes (Bukowski 2016):

- *Availability (AV)* – ability to be in state to perform the required functions under given work conditions, is described by:
    - *Reliability (REL)* – ability to perform the required functions, without failure, for a given time interval, under given work conditions;
    - *Maintainability (MAI)* – ability to be retained in, or restored to a state to perform as required, under given conditions of use and maintenance;
    - *Maintenance Support Performance (MSP)* – effectiveness of an organization in respect to maintenance support;
- *Safety (SA)* – ability to operate, normally or abnormally, without danger of causing human injury or death and without damage to the system's environment, it consists of:
    - *Absence of Critical Damages (ACD)*;
    - *Protection of the environment* against the effects of any potential critical damages *(PRO)*;
- *Security (SE)* – ability to prevent an unauthorized access to, or handling of system state, can be described by the concurrent existence of:
    - *Confidentiality (CON)* – unavailability to non-enabled persons;
    - *Integrity (INT)* – impossibility of introducing changes into the system by non-enabled persons;

  - *Accessibility for enabled users only (ACC)*;
- *Resilience (RE)* – a collective term describing the ability of a system to absorb and withstand the failure impact, and still continue to operate at acceptable predefined performance level, is described by:
  - *Absorbability (ABS)* – capability of a system to fulfil its function, in a timely manner, in the presence of failures (survivability);
  - *Recoverability (REC)* – capacity of a system to recover from a failure, within the acceptable time and costs limits (restoration);
  - *Adaptability (ADA)* – ability to adapt to changed working conditions (flexibility, agility, ability to learn).

Based on this structure of properties the dependability of a system, for a given time interval (t_1, t_2), can be described by the model:

$$D(t_1,t_2) = \{AV(t_1,t_2); SA(t_1,t_2); SE(t_1,t_2);\ RE(t_1,t_2)\} \quad (5)$$

This model can be interpreted as follows: *A system's dependability is the collective term that describes its ability to continuous, safe and secure fulfilment of the required functions in a risky environment.*

The availability attribute is a research object of an area of *reliability engineering*, the safety attribute belongs to *safety engineering*, and the security attribute is a subject of *security engineering*. All these areas of knowledge have been studied for several decades and are currently well developed. However, the fourth of the attributes - resilience - is presently under intensive research, and the field of *resilience engineering* is in constant development.

4. Modelling resilience using the service continuity approach

From the operational perspective, the typical 'mess' (see Ackoff et al. 2006) for complex engineered systems is caused by *losing the continuity of production or service processes*. This type of risk sources is called disturbance and can lead to disruptive event in a given system. The behaviour of the system in 'mess' situations depends to a large extent on system's structure and its operational features. Table I shows the summary of the basic operational features for the main types of systems. The basic issue for our consideration is the problem of how the system behaves in response to disturbances. We can distinguish four basic types of responses: resistance, robustness, absorption and recovery, as well as learning and adaptation.

Table I: The main types of systems and their operational features (based on Bukowski 2019)

Type	Complexity	State adjustment	Response to disturbances	Example
I - Passive	low	constant	resistance	elements
II - Reactive	medium	static control	robustness	parts
III - Responsive	high	dynamic control	absorption & recovery	subsystems
IV - Active	very high	smart control	learning & adaptation	SoS (e.g. CI)

In order to develop the resilience model of complex engineered systems we proposed the following basic definitions of the main terms:

- *Disruptive event (DE)* – an act of delaying or interrupting the process continuity (e.g. system failure, natural catastrophe, man-made fault).
- *Continuity (CON)* – a system capability to deliver products or services at acceptable, predefined performance level under the real work conditions (e.g. despite disruptive events *DE*).
- *Disruptive event impact (DEI)* – the degree to which a system is affected by a disruptive event *DE*.
- *Resilience to a disruptive event (RE)* – the ability of a system to absorb and withstand the disruption impact, and still continue to deliver products or services at acceptable predefined performance level, as well as the adapt-capacity to a new work conditions.
- *Resilience metric* - a collective term described by four main indicators: absorbability *(ABS)*, recoverability *(REC)*, adaptability *(ADA)* and disruptive event impact *(DEI)*.

Based on these assumptions we propose *the concept of service continuity oriented approach*. This concept is closely related to the ideas of resilient enterprise (Sheffi 2007) as well as business continuity management (British Standards Institute 2006). The model is based on a typical course of a service delivery process, interrupted by an occurrence of a disruptive event leading to a disruption of this process continuity. A quantitative interpretation of this model is shown in Figure 2. The thick line shows the course of an idealized system operation as it changes its performance in function of time. Prior to the occurrence of a disruptive event the system was functioning at the required level of performance *(P_{Req})*. The occurrence of a disruptive event *(DE)* is immediately followed by a sharp decline in system performance, until it reaches a minimum level of performance higher than a critical level of performance (P_{Min}>P_{Cri}). With the capacity to absorb the effects of a disruptive event, the system maintains its basic functions and gradually increases its performance. After the time t_4, it achieves a recovered performance level *(P_{Rec})*, which lies above the acceptable level of performance (P_{Rec}>P_{Acc}).The final phase of the course is characterized by the ability to adapt to new conditions, and as a result the system performance improves to the level *(P_{Ada})*.

Generally, there can be distinguished the following five fundamental phases in a typical course of a service delivery process with a continuity disruption (see Figure 2):

A. Resistant state – characterized by no reaction to small disturbances,
B. Robust behaviour – with short-term loss of performance after a disturbance and rapid return to the required state,
C. Absorption phase (*ABS*) - distinguished by ‘coping’ with disruption and continuity retain of operation,
D. Recovery phase (*REC*) - characterized by ‘bouncing back’ to acceptable performance level,

E. Adaptation phase (*ADA*) - distinguished by 'learning' from disruption and transformation to the new work conditions.

The resilience properties appear in the C, D, and E phases, so the disruption curve shape will be the basis for a quantitative evaluation of these properties. As shown in Figure 2, the loss of performance after a disruptive event *DE* is proportional to the area between the line showing the required performance and the actual course of the performance. Therefore, the quantitative measure for *disruptive event impact (DEI)* can be described as follows:

$$DEI = \langle L_{Dis} \rangle \tag{6}$$

where:
$L_{Dis} = \int_{t2}^{t5} \left[P_{Req} - P(t)\right] dt$ – expected loss of performance *P* caused by *DE*
P_{Req} – required performance level,
$P(t)$ – performance at the time t,
t_2 – beginning of disruption,
t_5 – end of disruption (return to required performance level).

The general model for resilience metric is represented as a collective term described by four dimensional vector as follows:

$$RE = \langle ABS, REC, ADA, DEI \rangle \tag{7}$$

with:
$ABS = \langle P_{Min}, T_{Abs} \rangle$ – absorbability (8)

$REC = \langle P_{Rec}, T_{Rec} \rangle$ – recoverability (9)

$ADA = \langle P_{Ada}, T_{Ada} \rangle$ – adaptability (10)

$DEI = \langle L_{Dis}, T_{Dis} \rangle$ – disruptive event impact (11)

where (see Figure 2):

P_{Min} – the lowest performance level during disruption (absorbability measure),
P_{Rec} – performance level after recovery (recoverability measure),
P_{Ada} – performance level after adaptation (adaptability measure),
P_{Cri} – the critical acceptable performance level during disruption (given for the process),
P_{Acc} – the acceptable performance level after disruption (given for the process),
$T_{Abs} = t_3 - t_2$: absorption time (t_3 – end of absorption phase),
$T_{Rec} = t_4 - t_2$: recovery time (t_4 – end of recovery phase),
$T_{Dis} = t_5 - t_2$: disruption time (t_5 – return to required performance level),
$T_{Ada} = t_6 - t_2$: adaptation time (t_6 – end of adaptation phase),
$T_{Cri} = t_{Cri} - t_2$: the critical acceptable disruption time (given for the process),
L_{Dis} – the expected loss of performance *P* caused by disruption event,

L_{Cri} – the critical acceptable loss of performance P caused by disruption event (given for the process).

Parameters marked as 'given for the process' are constant values, while all other parameters are random variables. Therefore, based on formulas (7) to (11) the resilience RE is a multidimensional random variable whose probability distribution is very difficult to evaluate in practice (and in many cases even impossible). So, for practical use, a simple rules-based resilience assessment system is proposed. An example of such a system is shown in Table II. The application of these rules can be shown on the example of the run from Figure 2, for which the values of main variable and constant parameters are given in brackets (e.g. P_{Min} = 20% > P_{Cri} = 10%), and disruption impact L_{Dis} is less than the critical limit L_{Cri}. In this case class II conditions are met, but class III is not achieved (because T_{Ada} > T_{Cri}), so *resilience level* can be considered as acceptable.

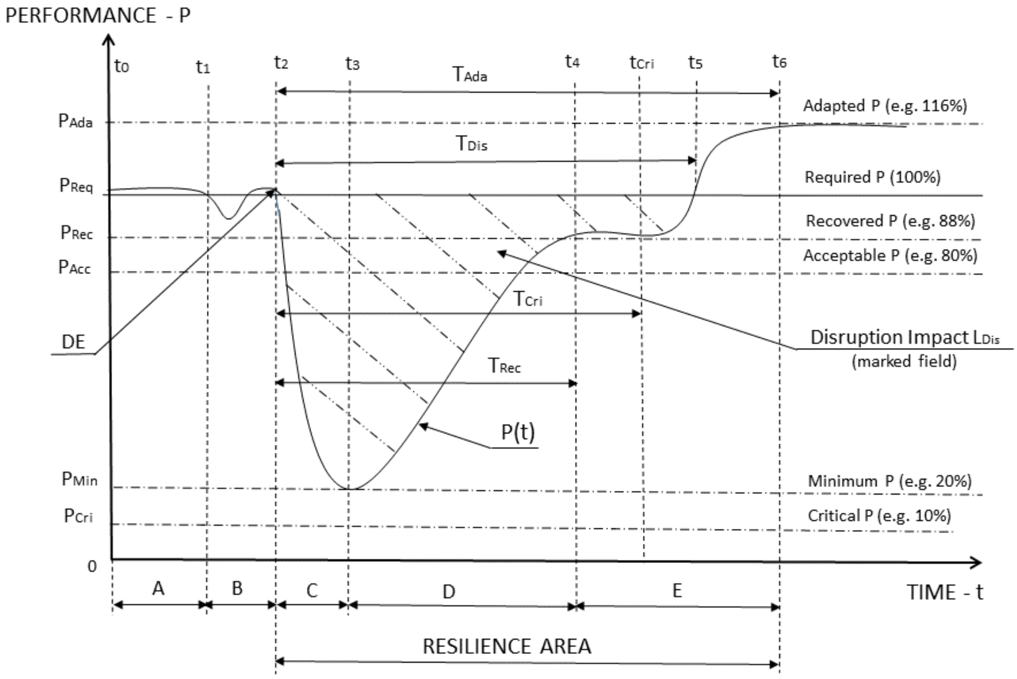


Figure 2. Exemplary course of a service delivery process with a continuity disruption (based on Bukowski 2019)

This type of evaluation system can be integrated into an existing risk management system, which can contribute to a significant improvement in dependability of the whole complex engineered systems, such as global logistics networks.

Table II. An evaluation system for resilience assessment of complex engineered systems - an example

Class	Resilience level	Requirements
I	Unacceptable	$P_{Min} < P_{Cri}$ *or* $P_{Rec} < P_{Acc}$ *or* $T_{Rec} > T_{Cri}$ *or* $L_{Dis} > L_{Cri}$
II	Acceptable	$P_{Min} > P_{Cri}$ *and* $P_{Rec} > P_{Acc}$ *and* $T_{Rec} < T_{Cri}$ *and* $L_{Dis} < L_{Cri}$
III	High	$P_{Min} > P_{Cri}$ *and* $P_{Rec} > P_{Acc}$ *and* $T_{Ada} < T_{Cri}$ *and* $L_{Dis} < L_{Cri}$
IV	Very high	$P_{Min} > P_{Cri}$ *and* $P_{Rec} > P_{Acc}$ *and* $T_{Ada} < T_{Cri}$ *and* $P_{Ada} > kP_{Req}$ *and* $L_{Dis} < L_{Cri}$

where: k - adaptability index (recommended value $k > 1$).

5. Conclusions

Based on the transdisciplinary review of publications related to resilience drawn from different areas of knowledge, as well as our own experience we propose the following statements:

- The term *resilienc*e can be used both in a narrow and broad perspective. In the case of complex engineered systems (e.g. system of systems type) a broad approach is appropriate; a concept based on two basic elements, namely *disturbance*s (uncontrollable changes), and *transformation* (adaptive ability to survive and turn unexpected changes into opportunities).
- In order to construct an *analytical model of resilience*, which allows for its quantitative evaluation, it is necessary firstly to define the object of deliberation and subsequently different threats that it may be subject to. This requires a *multidimensional approach*, both from the *operational perspective* (resources and processes) and from *the risk perspective* (threats and disturbances).
- For this purpose we developed *the service continuity oriented approach,* which is closely related to the ideas of *resilient enterprise* as well as *business continuity management*. The *resilience model* is based on a typical course of a service delivery process, interrupted by an occurrence of a disruptive event leading to a disruption of this process continuity.
- For quantitative evaluation of the complex systems resilience to a disruption risk we propose the *resilience metric* - a collective term described by four main indicators: absorbability, recoverability, adaptability and disruptive event impact.
- Based on the parameters of these metrics we can built an evaluation system for *resilience assessment* of different complex engineered systems. This kind of evaluation system can be *integrated into a general risk management system*, which can contribute to a significant *improvement in dependability* of any complex engineered system.

Summarizing, there seems to be a rational desire to create the knowledge domain of *Resilience Science* as the sum of experiences and concepts from different fields of knowledge in a transdisciplinary perspective. In this big picture *General Resilience* would mean a capacity to survive, recover and adapt in face of changes characterized by *deep uncertainty* as well as *unknown unknowns*.

References

Ackoff R.L., Magidson J., Addison H.J. (2006) *Idealized design: creating an organization's future*, Pearson Education

Aven T. (2011) On some recent definitions and analysis frameworks for risk, vulnerability and resilience. *Risk Analysis*; 31(4); 515–22

Avizienis A. et al. (2004) Basic concepts and taxonomy of dependable and secure computing, *IEEE Trans. on Dependable and Secure Computing*; 1(1); 11–33

Baida Z., Gordijn J., Omelayenko B. (2004) A Shared Service Terminology for Online Service Provisioning. In: *The 6th International Conference on Electronic Commerce*

British Standards Institute (2006) *PAS 56: Guide to business continuity management*, BSI, London

Bukowski L. (2016) System of Systems Dependability - Theoretical Models and Applications Examples, *Reliability Engineering & System Safety*, 151; 76-92

Bukowski L. (2019) *Reliable, Secure and Resilient Logistics Networks. Delivering products in a risky environment*, Springer International Publishing AG, ISBN 978-3-030-00849-9 (Hardcover), ISBN 978-3-030-00850-5 (eBook)

Christopher M., Peck H. (2004) Building the resilient supply chain, *The Int. Journal of Logistics Management*; (15), 2; 1-14

Dekker S. et al. (2008) Resilience Engineering: New directions for measuring and maintaining safety in complex systems, *Final Report December 2008*

EN ISO 9000:2015, Quality management systems – Fundamentals and vocabulary

EN ISO 9001:2015, Quality management systems – Requirements

ERISS (2016) Tilburg School of Economics and Management, *the ERI in Service Science*, http://www.tilburguniversity.nl/eriss/research/service/

Francis R., Bekera B. (2014) A metric and framework for resilience analysis of engineered and infrastructure systems, *Reliability Engineering and System Safety* 121; 90-103

Hollnagel E., Woods D.W., Leveson N., editors. (2006) *Resilience Engineering: Concepts and Precepts*. Ashgate, Abingdon, Oxon, GBR

Kröger W., Zio E. (2011) *Vulnerable systems*. Springer-Verlag, London

Park J., Seager T.P., Rao P.S.C. (2013) Convertono M., Linkov I. Integrating risk and resilience approaches to catastrophe management in engineering systems. *Risk Analysis*, 33,3; 356-367.

Peck H. (2006) Supply chain vulnerability, risk and resilience, in *Global Logistics*, 5th edition, editor D. Waters, Kogan Page, London

Pettit T.J., Croxton K.L., Fiksel J. (2013) Ensuring supply chain resilience: development and implementation of an assessment tool. *Journal of Business Logistics*, 34(1); 46-76.

Salvendy G., Karwowski W. (2010) *Introduction to Service Engineering*, Wiley, New Jersey

Sampson S.E. (2010) A unified service theory, in Salvendy, G. & Karwowski, W. *Introduction to Service Engineering*. Wiley, New Jersey

Sheffi Y, Rice Jr. JB. (2005) A Supply Chain View of the Resilient Enterprise. *MIT Sloan Management Rev*., 47; 41–48.

Sheffi Y. (2007) *The resilient enterprise: overcoming vulnerability for competitive advantage,* MIT Press, Cambridge

Waters D. (2007) *Supply chain risk management : vulnerability and resilience in logistics*, Kogan Page Limited, London & Philadelphia; 2007.

Westrum R. A. (2006) Typology of Resilience Situations, in *Resilience Engineering. Concepts and Precepts*, editors Hollnagel, E. Woods D.W., Leveson N., Ashgate Abingdon, Oxon, GBR

Models of information influence for assessing information systems security

Igor Goncharov, Nikita Goncharov, Pavel Parinov
JSC “NGO “Infosecurity”
St. Kukolkina, 9, 402
394018, Voronezh, Russia

Abstract

A new approach to the analysis of conflict interaction between information systems and intruders is suggested. The approach uses mathematical models based on hybrid automata formalism. An estimate of the probability of the intruder’s success is given. The paper also demonstrates that it is possible to abstract from the specific type of distribution density for the duration of each possible state of the parties of the conflict. A model of dissemination of destructive information influence within the information system is suggested. It shows the connection between the dissemination of destructive influence and the process of state transition of the information system subjects. An example of the analysis of dissemination of destructive information influence is given.

Key words: information systems security, hybrid automata, cellular automata, conflict modelling, modelling of information influence.

1. Introduction

When studying the security of information systems (IS) based on modern technologies, it is vital to consider two major groups of problems: violation of information security of the information system and possibility of dissemination of destructive information influence (DII) within the IS. In actual practice, these problems are interconnected and should be considered together. To provide for a comprehensive analysis we suggest two models: a model of conflict interaction between the information system and the intruder based on hybrid automata formalism, and a cellular automaton based model of dissemination of destructive information influence within the information system that takes into account the inner factors of the systems’ subjects and their condition.

2. Simulating conflict interaction between information systems and intruders

It is first necessary to determine a typical model of conflict interaction between an information system and an intruder. We suggest a model based on hybrid automata formalism that is used to determine the ratios for approximate estimate of probability of security violation and the lower bound of probability of security violation in the IS.

The model uses the most basic parameters such as mathematical expectation and variance for the duration of each of the discrete states of the IS and the intruder. The main features of hybrid automata and their application in simulating conflict interaction of systems were considered in the earlier works by the authors [1, 2].

Let us suppose that one of the parties (Party A) of the conflict is an information system (IS). The IS operates successfully, if it ensures the security of the information within itself in a set period of time $0 \le t \le T$. The IS itself is constantly in one of the states typical for its operation and functioning under normal conditions. The IS fails, if the security of the information within it is violated, at which point the system transfers to a corresponding critical state. The other party (Party B) of the conflict is an intruder system that aims to violate the security of the information within the IS and thus transfer the IS into the critical state within a set period of time. The intruder system succeeds, if it manages to reach this target. Party B fails, if it does not manage to violate the security of the information within the set period of time $0 \le t \le T$.

Fig. 1 presents two hybrid automata (HA) functioning simultaneously: automaton A and automaton B. For these automata the set of discrete variables $S^D = \{s_a, s_b\}$, which describe the most common states, is presented by two variables, each taking the values $s_a \in Q_A = \{L_A, D_A\}$, $s_b \in Q_B = \{L_B, D_B\}$ [3]. State L_A represents the functioning of A until the moment when the intruder takes advantage of the existing vulnerabilities, which results in security violation and transition of the IS to the critical state D_A (“failure” A). State L_B represents the functioning of B that aims to interfere with the operation of A, and lasts for a set period of time after which the intruder fails to breach the security of the information system (“failure” B) and transfers to the state D_B. Transition to D_A and D_B proceeds abruptly and is influenced by $attack\_B$ and $t \ge T$, leading to failure for A and B respectively.

To detail the operation of both parties of the conflict, it is necessary to consider the inner states of the set $L = \{L_A, L_B\}$ as embedded hybrid automata which we will refer to as hybrid automata of active elements (HA AE) [3, 4].

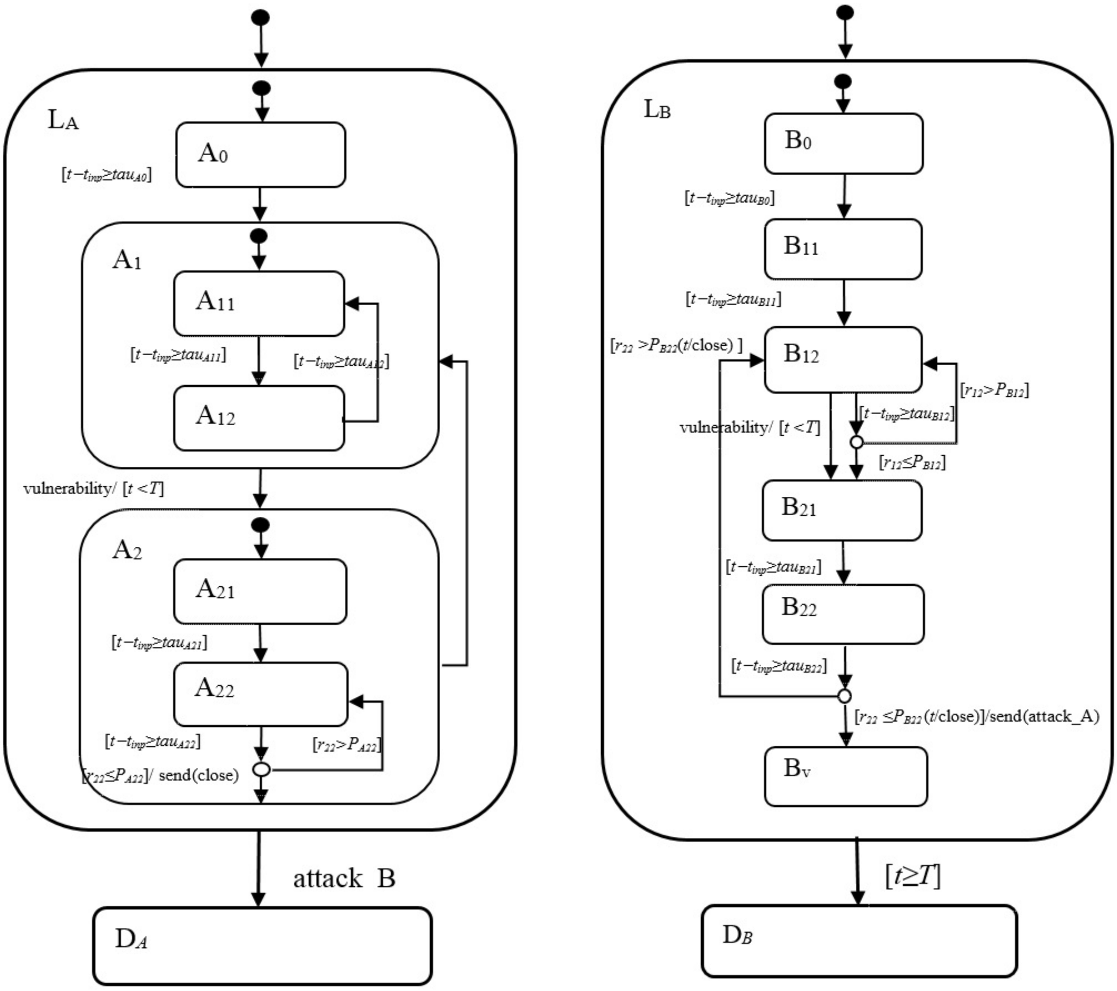


Figure 1 - A model of conflict interaction between the information system and the intruder based on hybrid automata

The subset of symbols $Q_{A0}^{L} = \{A_0\}$ consists of the symbol of the state that is responsible for getting system A into operation. The subset of symbols $Q_{A1}^{L} = \{A_{11}, A_{12}\}$ represents the system's operation under normal conditions. The symbols are embedded into general state A_1, which means that “system A is secure from all known vulnerabilities”. The subset of symbols $Q_{A2}^{L} = \{A_{21}, A_{22}\}$ represents the functioning of the system after a new vulnerability was found or appeared. The symbols are embedded into general state A_2, which means that “system A is insecure from a known vulnerability”. The transition from state A_1 to state A_2 is influenced by the event “vulnerability” under the condition that this vulnerability appears in the period of time $[t, T)$, set for conflict interaction between systems. To describe the way new vulnerabilities appear, we used a model of external random flow of events. Transition from state A_2 back to state A_1 is possible, if the system manages to eliminate the vulnerability in A_2. For active elements of party B the following states and transitions should be introduced when modelling the events of a typical conflict. The subset of symbols $Q_{B0}^{L} = \{B_0\}$ consists of the symbol of the state that is responsible for getting system B into operation. The preparatory actions do not repeat.

The subset of symbols $Q_{B1}^{L} = \{B_{11}, B_{12}\}$ represents the states of system B when it searches for and identifies the vulnerabilities, system A being in state A_1 (system A is secure from all known vulnerabilities). State B_{11} determines the functioning of the system aimed at gathering information about system A (analysis of the organisation principles, technical tools, and software, and rights and qualifications of the users and operating personnel). State B_{12} determines the way system B searches for vulnerabilities when system A operates under normal conditions. Probability P_{B12} is set by the operator of local behaviour as the probability of identification of a vulnerability when system A operates under normal conditions. It is time-independent. The model shown in Fig. 1 describes the main transition type as well as another type of transition from B_{12} into the following group of discrete states. The latter is determined by the event "vulnerability" (identification of a new vulnerability) happening in the period of time $[t, T)$. We assume that systems A and B receive the information about a new vulnerability at the same time. The subset of symbols $Q_{B2}^{L} = \{B_{21}, B_{22}\}$ represents the functioning of system B after a new vulnerability was detected. State B_{21} determines the actions performed to analyse the detected vulnerability and utilise it. The state is limited in time. State B_{22} activates the utilisation of the vulnerability in order to violate the security of system A. The subset of symbols $Q_{Bv}^{L} = \{B_v\}$ consists of the symbol of the state when the security of information in system A is successfully violated. The transition to the critical state is followed by the event attack_A, which transfers the HA of party A from state L_A into eigen state D_A. State B_v is absorbing for this model. Transition from state B_{22} back to state B_{12} is performed, if system B fails to utilise the detected vulnerability.

2.1. Assessing the probability of information security violation

Here we present the analytical relations obtained in the analysis of the probability of success of party B [1, 3] in a situation when it does not receive any external information about new vulnerabilities.

Analytical relation based on Gaussian approximation for a random variable $\tau_{b,1}$ [4, 5]:

$$\begin{aligned} P_{Bga}^{(1)} &= \Pr(0 < \tau_{B,1} < T) = \int_{0}^{T} N(u, m_{B,1}, d_{b,1})du = \\ &= F\left(\frac{T - m_{B,1}}{\sqrt{d_{B,1}}}\right) - F\left(\frac{-m_{B,1}}{\sqrt{d_{B,1}}}\right), \end{aligned} \tag{1}$$

$$F(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} N(v, 0, 1)dv \quad .$$

where $N(u, m, d)$ is the Gaussian probability density distribution with corresponding parameters.

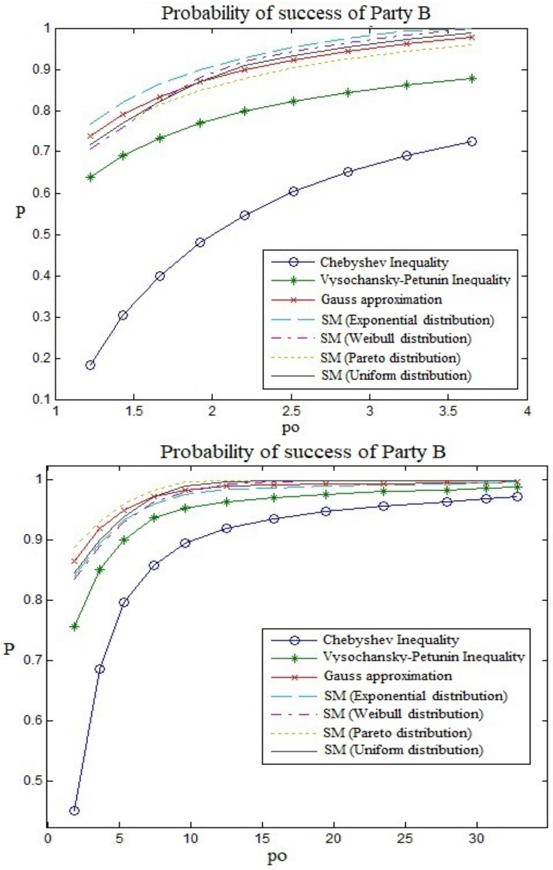
To estimate the lower probability of security violation, Chebyshev's inequality can be used [4]. The estimate can also be specified using the Vysochanskij–Petunin inequality [4, 5], assuming that the distribution density of composition $\tau_{b,1}$ is unimodal:

$$P_{Bvp} = \Pr\left[\tau_{B,1} < T\right] \geq \Pr\left[\left|\tau_{B,1} - m_{B,1}\right| < T - m_{B,1}\right] = \\ = \Pr\left[\left|\tau_{B,1} - m_{B,1}\right| < \frac{T - m_{B,1}}{\sqrt{d_{B,1}}}\sqrt{d_{B,1}}\right] \geq \qquad (2) \\ \geq 1 - \frac{4}{9\rho^2} = 1 - \frac{4d_{B,1}}{9(T - m_{B,1})^2}, \quad \rho = \frac{T - m_{B,1}}{\sqrt{d_{B,1}}} \geq \sqrt{\frac{8}{3}}$$

It is, however, much more difficult to estimate the probability of success of system B, if within the set period of time it receives information about a new vulnerability. The authors obtained analytical relations for this estimate as well, introducing a number of assumptions and approximations, but these results are out of the scope of the present paper.

2.2. Results of the experiment

We examined the possibility of using the obtained analytical relations by means of various types of distributions for the duration of each of the systems' states. In a series of statistical experiments, including 1,000 tests each, we considered various combinations of distribution laws, their parameters, and the probability of returning and repeating the tests. The obtained results were summarised as the dependencies of the probability of success P on the relation $\rho o = (T - m_{B,1})^2 / d_{B,1}$ [6, 7]. A few examples of such dependencies are shown in Figure 2.



a) *b)*

Figure 2 - Comparison of the obtained estimates with the results of simulation modelling

Fig. 2 demonstrates that using analytical relations based on Vysochanskij–Petunin inequality and Gaussian approximation allows for precise estimate of the lower probability and approximate estimates of probability of information security violation under the condition of ambiguity of probability density distribution within the duration of the respective states of the information system and the intruder system. Analytical relation based on Chebyshev's inequality yields rougher estimates. The precision of the analytical relations in each case is determined by preset parameters and the use of assumptions. Without specific assumptions, the margin of error introduced by the said analytical relations is offset by the possible errors of selecting the distribution law that may occur when the relations are strictly set.

The dependencies calculated for a specific IS and shown in Fig. 2 allow us to conclude that the larger the value of the parameter ρo, characterising the relative average difference between the duration of the conflict and the time needed for security violation, the higher the probability of security breach in the observed information system. This means that for preventive influence, time is more important than the probability of failure at the later stages of vulnerability search and utilisation.

3. Simulating dissemination of destructive information influence within the information system

When modelling and analysing the process of dissemination of DII we regarded the IS as a two-dimensional cellular automaton. A two-dimensional cellular automaton is a set of finite automata (subjects of the IS) allocated on the reference frame and marked with integer coordinates (i, j). Each automaton can have certain properties and be in one of the states $S_{i,j} \in \{S_1, S_2, .., S_k\}$. The state of a finite automaton (i, j) at a certain moment in time $t+1$ is determined as follows [8, 9]:

$$S_{i,j}(t+1) = F(S_{i,j}(t), N(i, j), t), \tag{3}$$

where F is the rule for the transition of state of the automaton; $N(i, j)$ is the point neighbourhood (i, j); t is a step on the axis of time.

In the cellular automaton model each cell changes its state while interacting with a limited number of other cells, normally adjacent ones with the same side or vertex. Therefore, it is easy to see the connection between the processes occurring on the micro level and the processes of spatial interaction between the elements [8].

To describe the process of dissemination of DII within the IS the following model is suggested. Information interaction within the IS is presented as a two-dimensional cellular automaton, whose grid is a two-dimensional array, where each cell is numbered with an ordered pair (i, j). Each cell is an information system subject. The nearest neighbours of each cell are considered the cells that have a common vertex with the one observed (Moore neighbourhood). Thus, each cell has 8 nearest neighbours. To eliminate the tip effect, the grid of the cellular automaton is topologically twisted into a torus [8], i.e. the first line is considered to be the continuation of the last one, and the last one precedes the first one. The same applies to the columns [9].

Each cell may be in one of the following states: S0 - initial state; S1 - the subject developed a reaction to the DII, but does not distribute it; S2 - the subject took in the DII, but does not disseminate it; S3 - the subject developed a reaction to the DII and distributes it; S4 - the subject took in the DII and disseminates it. Depending on the state and the inner properties, a cell may or may not disseminate the DII (by influencing the neighbouring cells). The state and behaviour of cells change according to the rules set for the suggested model. This rules consider the inner parameters of the IS subjects and their state. A state transition graph is presented in Fig. 3.

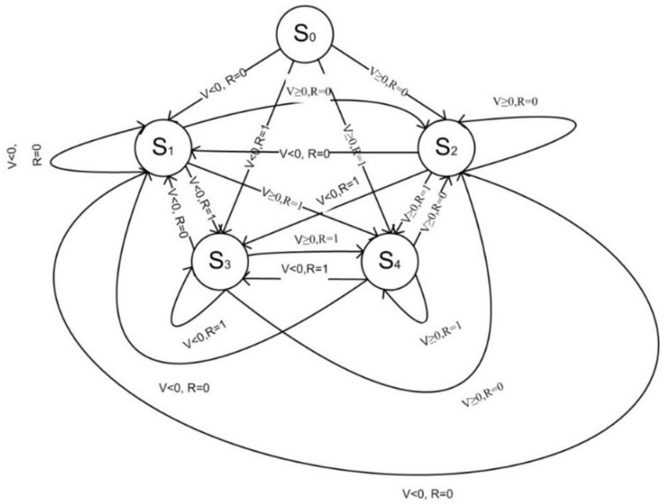


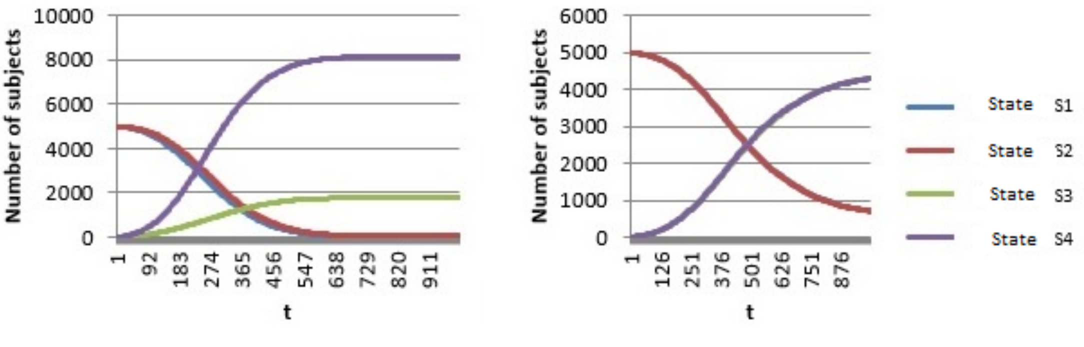
Figure 3 - State transition graph

The subject may either take in the destructive information influence or resist it. Depending on the inner parameters, the subject may also disseminate the DII within the IS, or not.

In our study we used the following modelling algorithm: initial stage - main properties of the IS subjects are determined; first stage (corresponds to the origin on the time axis) $t = 0$ - the whole grid consists of cells in state S_0, except for certain cells that initiate the DII; second stage - the DII is disseminated along the time axis $t = t + 1$, the inner parameters of the subjects are determined basing on the suggested model; cells with the value of DII dissemination equal 1 pass on the information to the neighbouring cells.

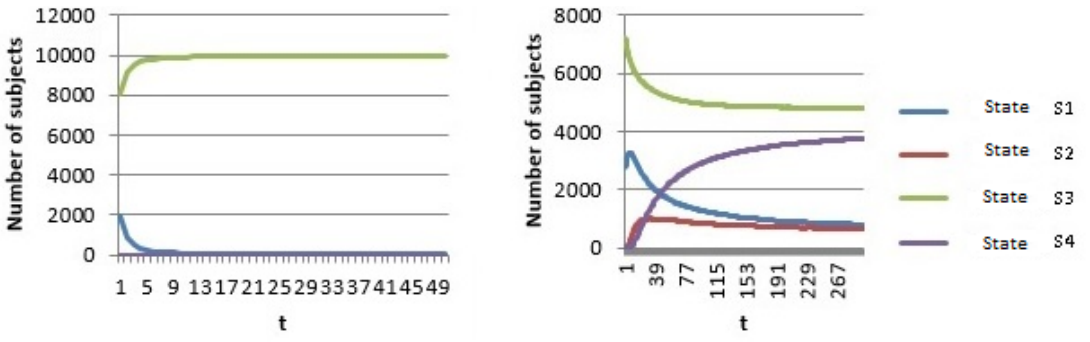
3.1 Results

Fig. 4 demonstrates the functioning of the automaton when most subjects are neutral to the DII. Fig. 5 demonstrates the functioning of the automaton when most subjects are negative to the DII. Fig. 6 demonstrates the functioning of the automaton when most subjects are positive to the DII. Figures "a" demonstrate the functioning of the automaton when the subjects take in the DII from other subjects. Figures "b" demonstrate the functioning of the automaton when the subject can resist the DII.



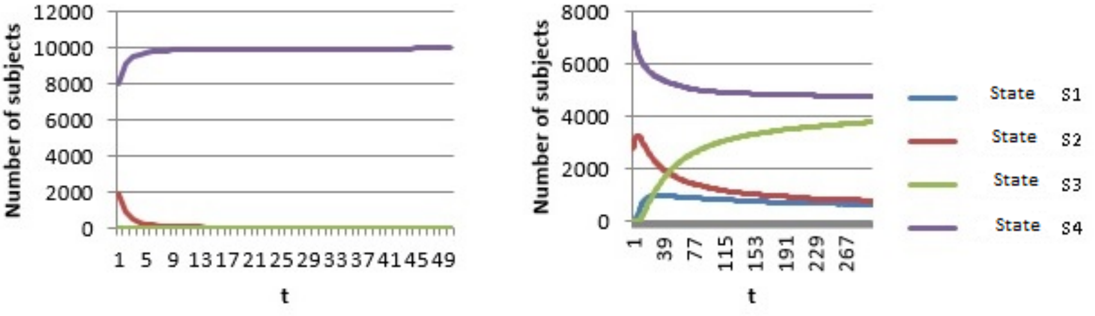
a b

Figure 4 - Distribution of cells according to the discrete time (most subjects are neutral to the DII)



a b

Figure 5 - Distribution of cells according to the discrete time (most subjects are negative to the DII)



a b

Figure 6 - Distribution of cells according to the discrete time (most subjects are positive to the DII)

Analysis of Figures 4-6 shows that
- the character of dissemination of the DII within the IS is practically exponential;
- when the subjects are neutral to the DII (Fig. 4a), just a small number of initiators can successfully perform the DII;
- when the subjects are negative or positive to the DII (Fig. 5a and 6a), the DII does not influence their state;
- when the subjects can resist the DII (Fig. 4B, 5b, and 6b), the number of subjects in states S3 and S4 is similar, irrespective of their initial state.

The suggested model demonstrates the connection between the process of dissemination of DII within the IS and the changes in the states of the IS subjects resulting from the interaction of interconnected subjects.

4. Conclusion

The suggested model of conflict interaction between the information system and the adversary, and the obtained analytical relations for approximate estimate of probability and lower probability of information security violation, demonstrates that it is not necessary to determine the specific type of distribution density for the duration of each possible state of the parties of the conflict. This model can be successfully applied to various problems concerning the security of ISs. The suggested model of dissemination of destructive information influence within the information system shows the connection between dissemination of destructing information influence and the process of state transition of the information system subjects. It is very important for studying security problems of information systems based on modern information technologies. Using both models together allows for a comprehensive study of the main factors effecting the security of modern information systems.

References

[1] Druzhinin, V.V. (1989) Introduction to the theory of conflict. *M.: Radio and Communication,* 288 p.

[2] Kolesov, Yu. B. (2012) Modeling systems. Dynamic and hybrid systems. Tutorial. *SPb.: BHV-Petersburg,* 224 p.

[3] Harel, D. Statechars (1987) A Visual Formalism for complex systems. *Science of Computer Programming - Vol.8.* pp. 231-274.

[4] Kolmogorov, A. N. (1976) Elements of the Theory of Functions and Functional Analysis. *M .: Science*. 544 p.

[5] Vysochansky, D. F. (1979) Justification of the R-sigma rule for unimodal distributions *Theory of Probability and Mat. Statistics*. *vol. 21.* pp. 23-35.

[6] Goncharov, N. I. (2018) Simulation of conflict interaction of systems using the formalism of hybrid automata. *Information Technologies - Moscow: New Technologies Publishing* House, No. 1, Volume 24. p. 17-27.

[7] Goncharov, N. I. (2017) Investigation of the conflict of coalition systems using the formalism of hybrid automata. *Vestnik VSU (system analysis and information technology)*. p. 56-70.

[8] Wolfram, Stephen (2002) A New Kind of Science. Champaign, *IL: Wolfram Media Inc.*, 1192 p.

[9] Goncharov, I. V. (2018) Modeling of processes of information and psychological influence in social networks. *Vestnik VSU (system analysis and information technology)*, pp. 93-104.

Igor Goncharov - Ph.D., CEO JSC “NGO “Infosecurity”

Nikita Goncharov - Information Security Specialist JSC “NGO “Infosecurity”

Pavel Parinov - Information Security Specialist JSC “NGO “Infosecurity”

On sensitivity of reliability and risk models to shape of their elements

N. Kuznetsov, G. Popov
125009, Moscow, Russia
International Union of Instrument&ICT Engineers
Tverskaya~St.12/2

V. Rykov
117198, Moscow Russia
Peoples Friendship University of Russia (RUDN University)
Miklukho – Maklays str. 6

Abstract

The problem of output characteristics for reliability and risk models to shapes of their input elements distributions is considered. Some classic results about strong and asymptotic insensitivity for these models and some recent investigations are mentioned. The project of further investigations are proposed.

Keywords: reliability and risk models, strong and asymptotic sensitivity.

1. Motivation and notations

Most of all Critical Infrastructures (CIs) sectors as well as threats to them contain essential random part such as reliability and risk. For CIs study, they should be represented as mathematical models, which will be models of stochastic systems. Input information for most of sectors Cis usually cannot be precisely found (mostly can be estimated statistically). Stability or insensitivity or weak sensitivity of system output system characteristics to their input parameters distributions is one of the key problem of whole natural sciences including CIs.

Thus, investigation of sensitivity of output system characteristics to shapes of their input information is a very important problem for such systems. In the talk, some examples of classic results about strong and asymptotic insensitivity of reliability and risk models output characteristics to their elements distributions are mentioned. Some recent results also will be considered and the problem for their development in framework of International Project will be proposed.

In the paper for reliability and risk models, we will use a little bit modified Kendall's notations [1]. Accordingly, to this notation any stochastic model is denoted with four symbols $(\alpha \mid \beta \mid \gamma \mid \delta)$, where

- α – symbol of an input flow;
- β – symbol of a service mechanism;
- $\gamma = (m, n)$ – symbol of the system structure where m is buffer size, n is number of servers;
- δ – symbol of service discipline.

For closed system (as well as reliability models) the round parenthesis “()” change to the angles “<>”. Each of these elements is also describes with their own model.

The paper is organized as follows. In the next section, some classical examples about insensitivity output characteristics of queueing systems and networks to shapes of their input information distributions will be remind. Next section deals with some known results about strong and asymptotic insensitivity in reliability models and some recent results in this direction. In the last section, some methodology for insensitivity in risk models is proposed. In conclusion, further investigations in the considered directions are proposed.

2. Classic results on sensitivity in queueing systems and networks

2.1 Erlang system

For Queueing System (QS) $(M \mid M \mid (0,n) \mid FIFO)$ with Poisson input flow of intensity α and exponentially distributed service time with mean β^{-1} consider a stochastic process.

$$J(T) = \text{number of busy servers at time } t$$

and define $\pi_j(t) = \mathrm{P}\{J(t) = j\}$. For steady states probabilities (s.s.p.) of the system

$$\pi_j = \lim_{t\to\infty} \pi_j(t)$$

Erlang [2] found the formula

$$\pi_j = \lim_{t\to\infty} \pi_j(t) = \frac{\rho^j}{j!}\left[\sum_{0\le i\le n} \frac{\rho^j}{j!}\right]^{-1} \tag{1}$$

where $\rho = \alpha\beta^{-1}$.

In 1975 B.A. Sevast'yanov [3] generalize this result and prove that the s.s.p. of the Erlang's system exists for any service time distributions $B(x)$ with finite mean $b = \int (1 - B(x))dx < \infty$, and Erlang's formulas (1) for them hold with $\rho = \alpha b$.

Thus, Sevast'yanov's theorem means that the Erlang's system s.s.p. insensitive to the shape of its service time distributions with fixed their mean value.

2.2 Open networks

For s.s.p. of open Stochastic Network (SN) (*M* ǀ *M* ǀ (*n*,*Q*) ǀ *FIFO*), consisting of r QS $S_1, S_2, ..., S_r$ with transition matrix $Q = \left[q_{ij}\right]$ Jackson [4,5] in 1957 obtained the following result.

Under condition $\lambda_i < n_i\beta_i$ for all $i = \overline{1,r}$ the s.s.p. of the open SN has the **product form**

$$\pi(j_1, ..., j_r) = \prod_{1 \le i \le r} \pi_{ji}^{(i)}, \tag{2}$$

where $\pi_{ji}^{(i)}$ are s.s.p.'s of the i-th node $(M \,|\, M \,|\, n_i \,|\, FIFO)$ with input intensity λ_i, which is solution of the equation

$$\lambda' = \alpha' + \lambda' Q^0, \tag{3}$$

such that $\lambda_i < n_i\beta_i$ for all $i = \overline{1,r}$, and

- $\overset{\text{uı}}{\alpha}\,'$ is the vector with components $\alpha_i = \alpha q_{0i}$, and
- $Q^0 = \left[q_{ij}^{(0)}\right], (i, j = \overline{1,r})$ is the matrix of the calls transmission between subsystems (sub-matrix of matrix Q without the first row and column).

At that s.s.p.'s of the i-th node given by

$$\pi_j = \begin{cases} \dfrac{\rho^j}{j!}\pi_0, \; j = \overline{1,n} \\ \dfrac{\rho^n}{n!}\left(\dfrac{\rho}{n}\right)^{j-n}\pi_0, \; j > n \end{cases}$$

and

$$\pi_0 = \left(e_n(\rho) + \frac{\rho^n}{n!}\frac{\rho}{n-\rho}\right)^{-1}.$$

2.3 Closed networks

For closed SN < *N* ǀ *M*$_r$ ǀ n_r,*Q* > consisting of r nodes, in which *N* calls served analogous result has been found in 1967 by Gordon and Newell [6].

If Q is a non-decomposable stochastic matrix of $r-1$-st rang, so the system s.s.p.'s have the **product form**

$$\pi(j) = \pi(j_1, ..., j_r) = G^{-1}(N, r)\prod_{1 \le i \le r} \frac{z_i^{ji}}{\beta_i^{ji} B_i(ji)}, \tag{4}$$

where

- z_i are the solution of *traffic equation*

$$\sum_{1 \le i \le r} z_i q_{ij} = z_j \tag{5}$$

- the functions $B_i(k)$ are determines recursively

$$B_i(0) = 1, \;\; B_i(j) = \min(j, n_i) B_i(j-1),$$

- the normalizing coefficient is

$$G = G(N,r) = \sum_{k \in E(N,r)} \prod_{1 \le i \le r} \frac{z_i^{ji}}{\beta_i^{ji} B_i(ji)} \tag{6}$$

2.4 BCMP Theorem

The above results have been obtained under assumption about Poisson input flow and exponentially distributed service times. So called **BCMP theorem** [7] mark out the conditions for class of networks (open, closed and mixed) with Poisson input, the s.s.p. of which admit product form representation for general service time distributions in nodes.

Thus, the BCMP-theorem can be treated as a statement about insensitivity of the network s.s.p. to the shapes of service time distributions in the system nodes up to their mean values.

3. Reliability models

3.1 Strong insensitivity

In 1976 I.Kovalenko [8] found the necessary and sufficient conditions for insensitivity of stationary reliability characteristics of redundant renewable system $< M_n \,|\, GI \,|\, m \,|\, FIFO >$ with exponential life time and general repair time distributions of its components to the shape of the latter. These conditions consist in sufficient amount of repairing facilities $m = n$, i.e. in possibility of immediate start to repair any of failed elements.

The sufficiency of this condition for the system with general life and repair times distributions $< GI_n \,|\, GI \,|\, m \,|\, FIFO >$ has been found in [9] with the help of multi-dimensional alternative processes theory. However, in the case of limited possibilities for restoration these results do not hold.

3.2 Asymptotic insensitivity

On the other hand in series of work of B.V. Gnedenko, A.D. Solov'ev [10-12] and others it was shown that under ``quick" restoration the reliability function of a cold standby double redundant heterogeneous system tends to the exponential one for any life and repair time distributions of its elements. This result also means the asymptotical insensitivity of the reliability characteristics of such system to the shapes of their elements life and repair times distributions.

In series of our papers [13-15] the problem of systems' steady state reliability characteristics sensitivity to the shape of life and repair time distributions of its components for the double redundant renewable systems $< GI_2 \,|\, GI \,|1|\, FIFO >$ has been considered, for the case, when one of the input distributions (either of life or repair time lengths) is exponential. For these models, explicit expressions for stationary probabilities have been obtained. For the system $< M_2 \,|\, GI \,|1|\, FIFO >$ they have form

$$\pi_0 = \frac{\tilde{b}(\alpha)}{\rho + \tilde{b}(\alpha)}, \quad \pi_1 = \frac{1 - \tilde{b}(\alpha)}{\rho + \tilde{b}(\alpha)}, \quad \pi_2 = \frac{\alpha b - (1 - \tilde{b}(\alpha))}{\rho + \tilde{b}(\alpha)}. \tag{7}$$

For the system $< GI_2 \,|\, GI \,|1|\, FIFO >$ they have dual form

$$\pi_0 = \frac{\rho^{-1} - (1 - \tilde{\alpha}(\beta))}{\rho^{-1} + \tilde{\alpha}(\beta)}, \quad \pi_1 = \frac{1 - \tilde{\alpha}(\beta)}{\rho^{-1} + \tilde{\alpha}(\beta)}, \quad \pi_2 = \frac{\tilde{\alpha}(\beta)}{\rho^{-1} + \tilde{\alpha}(\beta)}. \tag{8}$$

These formulas show the **evident sensitivity** of the s.s.p. to the shapes of non-exponential distributions in the form of their Laplace-Stiltjes transforms. However under rare failures (as well as under quick restoration) as it was shown in [13,16] this sensitivity become vanishingly small. The numerical investigation and simulation results, given in [17,18] demonstrate enough quick appearance of practical insensitivity of the time dependent as well as stationary reliability characteristics to the shapes of life and repair time distributions with fixed their mean values.

In [19] these results have been generalised for heterogeneous systems and in [20] for systems with dependent failures.

4. Insensitivity in risk models

For reliability of complex system investigation in the middle of 60-th last century in Bell Lab it was proposed to use the **fault tree**. Later the same methods has been used also for the risk models investigation. There is wide literature, devoted to this problem (including also computer tools for the methods applications).

Based on this approach in a recent book [21] it was proposed methods for complex risk events analysis. It is based on

- risk tree construction and its structure function calculation,
- risk tree rigging with initial information,
- main risk parameters calculation,
- sensitivity of risk indexes to input information investigation, and
- critical paths accordingly to different criteria in risk tree finding.

The details of this approach in the talk will be done. Some Program for realization of this approach as a special computer tools for wide application in practice is proposed.

5. Conclusion

In the talk the problem of sensitivity analysis of output characteristics for reliability and risk models to shapes of their input parameters distributions is proposed. Examples of some classic results about strong and asymptotic insensitivity of such models are remind. Some recent results in this direction for reliability models has been done. Further development of the ideas of insensitivity of reliability and risk models is proposed.

Acknowledgements

The publication was financially supported by the Ministry of Education and Science of the Russian Federation (the Agreement number 02.A03.21.0008) and by the Russian Foundation for Basic Research according to the research projects No. 17-07-00142 and No. 17-01-00633.

References

[1] D.G. Kendall. Stochastic processes occurring in the theory of queues and their analysis by the method of embedded Markov chains. \\ Annals of Math. Stat., 1953. Vol 24. P. 338-354.

[2] Brockmeyer E., Halstrom H.L., Ensen A. The Life and Works of A.K. Erlang. Copenhagen: 1948.

[3] B.A. Sevast'yanov. An Ergodic Theorem for Markov Processes and Its Application to Telephone Systems with Refusals. Theory of Probability and its Applications, Vol. 2, No. 1, 1957.

[4] J.R. Jackson (1957). Networks of waiting lines. // Oper. Res. 1957, 5, No. 4, 518-521.

[5] J.R. Jackson (1963). Jobshop-like queueing systems. //Manag. Sci. 1963, 10, No. 1, 131-142.

[6] W.J. Gordon, G.F. Newell (1967). Closed queueing systems with exponential servers. // Oper. Res. 1967, 15, No. 2, 254-265.

[7] F. Baskett, K.M. Chandy, R.R. Muntz, F.D. Palacios (1975). Open, closed and mixed networks of queueswith different classes of customers. // J. Assoc. Mach., 1975, 22 No. 2, 248-260.

[8] I.N. Kovalenko. Investigations on Analysis of Complex Systems Reliability. Kiev: Naukova Dumka, 1976. - 210 p. (In Russian).

[9] V. Rykov. Multidimensional Alternative Processes as Reliability Models. Modern Probabilistic Methods for Analysis of Telecommunication Networks. (BWWQT 2013) Proceedings. Eds: A.Dudin, V.Klimenok, G.Tsarenkov, S.Dudin. Series: CCIS 356. Springer, 2013. P.147-157.

[10] B.V. Gnedenko. On cold double redundant system. // Izv. AN SSSR. Texn. Cybern. No. 4 (1964), P. 3–12. (In Russian).

[11] B.V. Gnedenko. On cold double redundant system with restoration. // Izv. AN SSSR. Texn. Cybern. No. 5 (1964), P. 111 –– 118. (In Russian).

[12] A.D. Solov'ev. On reservation with quick restoration. // Izv. AN SSSR. Texn. Cybern. No. 1 (1970), P. 56–71. (In Russian).

[13] V. Rykov, Tran Ahn Ngia. On sensitivity of systems reliability characteristics to the shape of their elements life and repair time distributions. // Vestnik PFUR. Ser. Mathematics. Informatics. Physics. No.3 (2014), P. 65-77. (In Russian).

[14] D.Efrosinin, V.Rykov. Sensitivity Analysis of Reliability Characteristics to the Shape of the Life and Repair Time Distributions. In: Communication in Computer and Information Science, Vol. 487, pp. 101-112.

[15] Dmitry Efrosinin, Vladimir Rykov and Vladimir Vishnevskiy. Sensitivity of Reliability Models to the Shape of Life and Repair Time Distributions. (9-th International Conference on Availability, Reliability and Security (ARES 2014), p.430- 437. Published in CD: 978-I-4799-4223-7/14, 2014, IEEE. DOI 10.1109/ARES 2014.65.

[16] D.V. Kozyrev. Analysis of Asymptotic Behavior of Reliability Properties of Redundant Systems under the Fast Recovery. // Bulletin of Peoples' Friendship University of Russia. Series ''Mathematics. Information Sciences. Physics" No.3 (2011), pp.49–57. (In Russian).

[17] V. Rykov, D. Kozyrev. On sensitivity of steady state probabilities of a cold redundant system to the shape of life and repair times distributions of its elements. // In: Proceedings of the Eights International Workshop on Simulation (Vienna, September 21st – 25th, 2015).

[18] V Rykov, D Kozyrev, E Zaripova. Modeling and simulation of reliability function of a homogeneous hot double redundant repairable system// Proceedings 31st European Conference on Modelling and Simulation (ECMS 2017), May 23rd-26th, 2017. Pp. 701-705.

[19] V. Rykov, D. Kozyrev. Analysis of renewable reliability systems by Markovization method. // Analytical and Computational Methods in Probability Theory and its Applications (ACMPT2017): Moscow, RUDN University, 2017. – P. 727 - 734.

[20] D. Kozyrev, N Kolev and V. Rykov (2018). Reliability Function of Renewable System under Marshall-Olkin Failure Model.// Reliability: Theory and Applications. Vol. 13, No 1 (48) March 2018, pp. 39-46.

[21] V. Rykov (2016) reliability of Engineering Systems and tehnological Risks. ISTE, Wiley, 2016,212pp.

Using advanced data analysis to learn from infrastructure databases: The case of the US National Bridge Inventory

Filippos Alogdianakis, Dimos C. Charmpis and Ioannis Balafas
Department of Civil and Environmental Engineering, University of Cyprus,
75 Kallipoleos Str., P.O. Box 20537, 1678 Nicosia, Cyprus

Abstract

Various infrastructure information is gathered nowadays in databases, which have become rather large after years of development and data collection. For thorough search and broad exploitation of the available information, even beyond its original scope, advanced data analysis approaches need to be employed. The present work is concerned with the exploitation of the data in the US National Bridge Inventory (NBI) maintained by the Federal Highway Administration (FHWA), which includes information for over 500,000 bridges. The information provided in NBI was analysed in combination with additional data from other sources (for climatic conditions, earthquake hazard, etc.). Where needed, data were converted to correspond to bridge locations using spatial interpolation techniques. Then, Exploratory Data Analysis (EDA), Analysis of Variance (ANOVA) and regression analysis methods were utilized to study the causes of bridge deterioration. These statistical methods yield quantitative results and allow the identification, ranking and measurement of intensity of factors contributing to the decrease of the structural condition of bridges with time.

Keywords: deterioration; spatial interpolation; exploratory data analysis; analysis of variance; regression analysis.

1. Introduction

Today's society relies on data collected from multiple sources, which are combined and processed to produce information that assists decision making at various levels, ranging from everyday life to very specialized cases. All these processes can be included in the broad term of 'Data Analysis', which refers to various tools, such as data visualization, hypothesis testing and other statistical methods, that are employed to handle samples and select the most appropriate variables for modelling reality.

Infrastructures, and more specifically bridges, are exposed to various factors that could worsen their structural condition. When reliable data are available, a data analysis process can confirm or challenge building practices and design processes already applied, but also assist in modelling deterioration by identifying factors affecting it.

In many countries, inspections are performed on bridges to monitor the infrastructure's stock condition. The US Federal Highway Administration maintains an up-to-date National Bridge Inventory (NBI), which includes over 500,000 bridges in US territory. The NBI contains a considerable amount of information; this includes 116 coded items to describe each bridge, its characteristics, its condition, etc. [1]. An updated NBI is published annually, as each bridge must be inspected visually biennially. Bridge condition ratings are recorded on a scale 0-9, with 9 representing 'excellent' and 0 'failed' conditions. Inspections are carried out by qualified personnel complying with standard procedures set out in National Bridge Inspection Standards (NBIS) [1].

The NBI has been used by several researchers to investigate structural deterioration and material performance for bridges. In the various statistical methods utilized for this task, the explanatory variables have been usually selected by expert judgement [2,3]. Such approaches may derive erroneous models due to the neglect of other variables, which may be affecting structural deterioration more. Another common practice usually employed is the utilization of bridge data for only one individual State of the US and inclusion in the assessment of additional explanatory variables, such as weather data and other data available from GIS [4]. In these cases, although maintenance policies and acquired data can be considered uniform, the limited variation of exposure factors can lead to modelling errors. On the other hand, when utilizing the whole US bridge sample, many exposures have to be taken to account and not including them in the analysis may also lead to misleading results due to unjustified averaging. Furthermore, questions arise regarding the effect of typical factors suggested by experts, which have already been taken to account during the design process. Thus, a process is needed to formally select the variables, which should be incorporated in modelling structural deterioration. Recently, some data analysis procedures have started to be utilized, in order to select among factors affecting deterioration. Relevant efforts either include limiting assumptions for the factors considered [5] or study an individual State and consider only NBI factors [3].

In this paper, NBI data for the conterminous US States are utilized to study the factors affecting the superstructure condition of bridges. To enable this, it is assumed that hazard-driven maintenance and rehabilitation policies are predominant and that the effect of potential State policies can be neglected. Additional reliable sources were used, such as National Oceanic and Atmospheric Administration (NOAA) for climatic data [6] and United States Geological Survey (USGS) for earthquake hazard data [7]. These were combined with NBI data using spatial interpolation methods. Data analysis procedures were utilized to explore the data and attain an appropriate model for the combined dataset, whose main purpose is to reveal predominant factors affecting structural condition.

2. The data analysis process

Data analysis is a broad term used to describe a set of procedures utilized to process data, comprehend and quantify their important relationships and finally generate models that aim to describe reality. The data analysis process followed herein is graphically summarized in Figure 1. Initially, various relevant data collections (from

NBI, NOAA, USGS) are utilized to attain the necessary information. From each dataset, a number of variables are selected and filtered to exclude unwanted information (i.e. bad records, outliers, etc.), a process performed with the aid of Exploratory Data Analysis (EDA), whose tools are mainly graphical and assist the analyst in identifying problematic/unexpected features [8]. The filtering process is repetitive and ends when the datasets are clear from outliers or errors, which could affect the actual data analysis that follows.

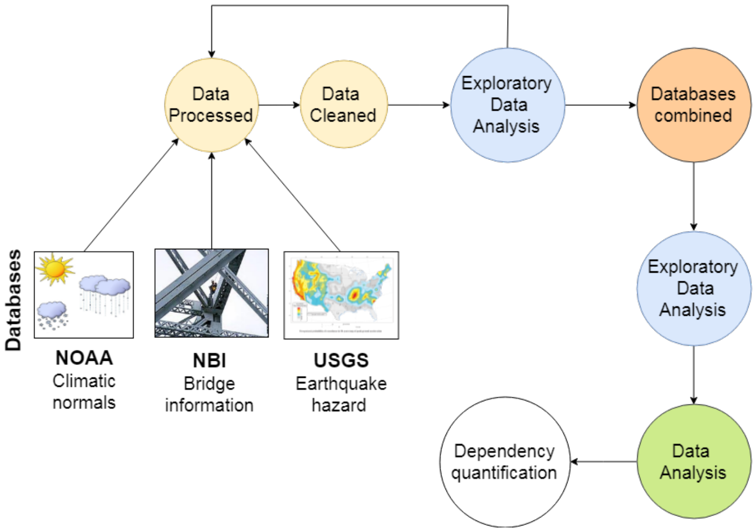


Figure 1. The data analysis process.

The cleaned datasets are then combined and EDA is once again performed to show variable distributions and intercorrelations, as well as to assist the analyst in selecting the appropriate data analysis methods to utilize [8]. The data analysis performed herein employs statistical modelling tools, such as Analysis of Variance (ANOVA) and regression analysis, which unveil and quantify relationships between the variables considered. Only parts of the conducted data analysis are presented. Specifically, initial variable selection, its filtering and the process of combining the different datasets are briefly discussed. Then, main EDA results are given, followed by the most important findings of ANOVA and indicative results of the regression analysis.

3. Formation of the analyzed dataset

Structural deterioration of bridges is linked to corrosion, which depends on various factors, such as temperature, aggressive chemicals (i.e. deicing salts, sea chlorides), freeze-thaw cycles, wet-dry cycles, among others [9]. Furthermore, accidental factors, such as earthquake hazard/action, are also important, as they dictate the implemented design standards and may add sudden induced damage to gradual/continuous deterioration. In this paper, to investigate deterioration, bridge characteristics, properties and current structural condition were extracted from the NBI, while climatic and earthquake attributes at bridge locations were obtained from NOAA and USGS, respectively.

The set of variables considered are presented in Figure 2. The variables are grouped based on the database they were extracted from and the variable type. Hence, the dependent variable is actually the product of evaluation (i.e. structural condition rating), while the independent variables offer information regarding bridges and potential deterioration factors. Further categorization was performed in numerical or categorical variables according to the form of information contained. Moreover, categorical variables were grouped in ordinal and nominal ones.

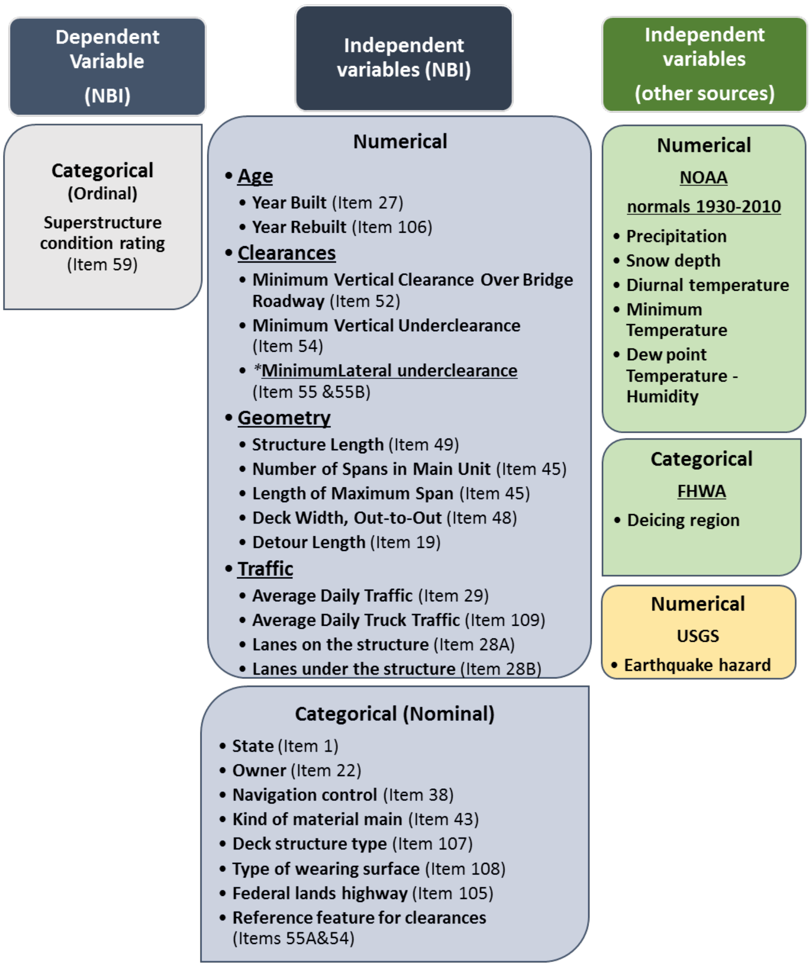

Dependent Variable (NBI)
Categorical (Ordinal)
Superstructure condition rating (Item 59)
Independent variables (NBI)
Numerical
• Age
• Year Built (Item 27)
• Year Rebuilt (Item 106)
• Clearances
• Minimum Vertical Clearance Over Bridge Roadway (Item 52)
• Minimum Vertical Underclearance (Item 54)
• *MinimumLateral underclearance (Item 55 &55B)
• Geometry
• Structure Length (Item 49)
• Number of Spans in Main Unit (Item 45)
• Length of Maximum Span (Item 45)
• Deck Width, Out-to-Out (Item 48)
• Detour Length (Item 19)
• Traffic
• Average Daily Traffic (Item 29)
• Average Daily Truck Traffic (Item 109)
• Lanes on the structure (Item 28A)
• Lanes under the structure (Item 28B)
Categorical (Nominal)
• State (Item 1)
• Owner (Item 22)
• Navigation control (Item 38)
• Kind of material main (Item 43)
• Deck structure type (Item 107)
• Type of wearing surface (Item 108)
• Federal lands highway (Item 105)
• Reference feature for clearances (Items 55A&54)
Independent variables (other sources)
Numerical
NOAA normals 1930-2010
• Precipitation
• Snow depth
• Diurnal temperature
• Minimum Temperature
• Dew point Temperature - Humidity
Categorical
FHWA
• Deicing region
Numerical
USGS
• Earthquake hazard

Figure 2. Variables considered in the data analysis.

3.1 NBI variable selection and filtering

A total of 25 variables (Figure 2) were selected from the NBI database regarding bridge superstructure condition, age, clearances, geometry, traffic (numerical variables), as well as ownership, water presence under the bridge, traffic type over and under the bridge (categorical variables). Of the total 614,387 structures included in the NBI database, not all were of interest in this study, therefore certain criteria were used to exclude e.g. culverts or bridges made of timber or stone. The exclusions performed regarded 166,750 structures, leaving a remaining population of interest of 447,637 bridges with year of construction after 1900 and specific utilized materials (reinforced/prestressed concrete, structural steel).

3.2 Climatic data

Structures are affected in the long term by local weather conditions, therefore the most appropriate respective data to take into account are the 'climatic normals'. NOAA manages and maintains a relatively dense network of weather stations all over the US and sustains a large collection of climatic and weather data. The US climatic normals are average values of climatological variables over a 30-year period (1981-2010) characterizing the conditions at each location [6]. The climatic normals utilized herein were: annual precipitation/rainfall, days of snow depth above 1 inch in a year, monthly average minimum temperature, monthly diurnal temperature range, hourly dew point temperature. The data were filtered for errors and processed to transform monthly and hourly data to annual ones. Furthermore, calculations were performed to attain values for annual average temperature and humidity.

3.3 Deicing region limits

Climatic data affect also the users of a bridge, inducing interventions to prevent accidents that may accelerate corrosion. Such is the case of deicing salts spread on the road surface to prevent frost. Deicing salts can be effective if snow depth is less than few centimeters. Thus, the FHWA map of US regions, where deicing is allowed, was copied as an image [10] and, using Google Earth, the coordinates of deicing region limits were identified, to be included in the analysis as complimentary data to the climatic variable of snow depth above 1 inch.

3.3 Earthquake hazard data

Earthquake resistance is a crucial attribute for a structure's service life in a seismic region. Seismic damage to bridges results usually from complex effects by various contributing variables that interact together. Peak ground acceleration (PGA), usually measured in terms of the acceleration of gravity (g), is the main variable typically used to represent the intensity of ground motion [11], although the seismic effect can be magnified by other factors. Seismic hazard maps are a product of analysis that considers past faults and earthquakes, behavior of seismic waves travelling the crust and near-surface site conditions [7]. Such maps are available from USGS, as derived from analyzing data from the whole US network. The seismic hazard expressed as the PGA with 2% probability of exceedance in 50 years was chosen to be incorporated in the analysis process. Relevant data were downloaded from USGS [7] for the conterminous US in the form of PGA values at gridded data-points (every 6 km) that formed a dense network of calculated hazard locations.

3.4 Combining the datasets

The aforementioned non-NBI databases offered information at locations, where data had been collected (weather stations) or calculated (grid of PGA values). To assign the corresponding climatic and earthquake hazard values to bridge locations, two different interpolation methods were utilized. Specifically, ordinary kriging interpolation was used for climatic data, as it is preferred for climatic and weather information [12]; linear interpolation for the densely gridded data of USGS was selected among the suggested methods by USGS. Results for two characteristic cases are presented in Figure 3.

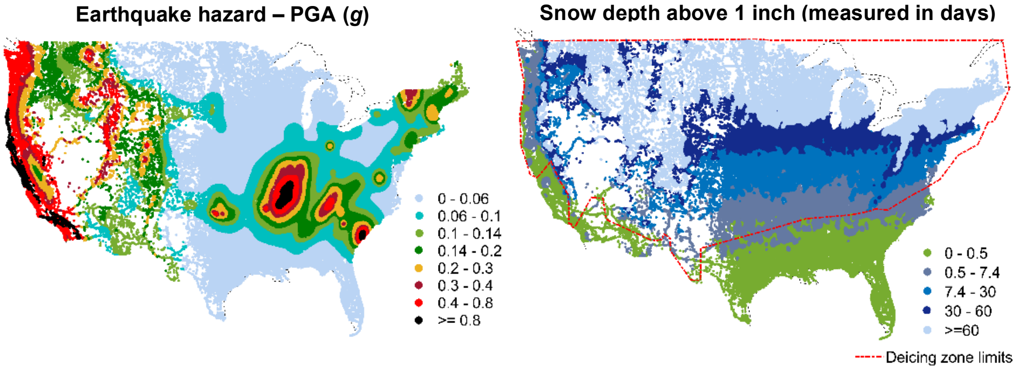


Figure 3. Maps of interpolated values regarding snow depth (kriging interpolation) and earthquake hazard (linear interpolation) at bridge locations.

4. Exploratory Data Analysis (EDA)

The EDA conducted for the whole sample included histograms and charts to visualize and explore distributions and frequencies of all selected variables. Additionally, correlograms were utilized to investigate the existence of statistical dependences among the variables.

Correlation is a statistical measure that shows whether and how strongly pairs of variables are statistically related. In particular, the Pearson correlation coefficient, which takes absolute values between 0 (no correlation) and 1 (full correlation), reveals how close two variables are to having a linear relationship with each other. Weak correlations are usually associated with absolute values in the range 0-0.65, moderate in the range 0.65-0.75, while strong correlations correspond to coefficients taking values higher than 0.75. A negative correlation value indicates that the two variables are negatively correlated. In Figure 4, correlation results are represented circles of appropriate size and color intensity. Specifically, larger circles with intense colors reveal stronger correlations, while small circles with faded colors weaker correlations. The color map given allows negative or positive correlations to be distinguished. The reported correlation results were calculated only for numerical variables.

The correlation analysis was conducted separately for NBI-based independent variables (regarding bridge characteristics and properties) and for independent climatic and earthquake hazard variables. The results for NBI independent variables (Figure 4(a)) showed that there are mostly weak correlations among them. Exceptions were geometric variables measuring similar properties (deck width and lanes on a structure; length and maximum spans). On the other hand, independent climatic and earthquake hazard variables (Figure 4(b)) showed strong correlations among the different temperatures and days of snow depth above 1 inch.

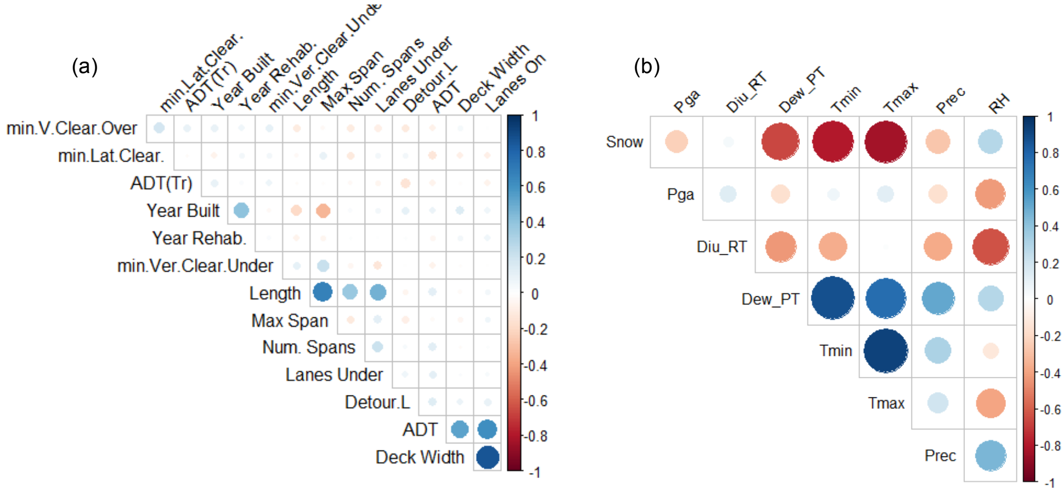


Figure 4. (a) Correlogram of independent NBI variables (min vertical clearance over bridge, min lateral clearance, average daily truck traffic, year built, year rehabilitated, min vertical under clearance, length, max span, number of spans, lanes under bridge, detour length, average daily traffic, deck width, lanes on bridge). (b) Correlogram of independent climatic (non-NBI) variables (snow depth above 1 inch, PGA – earthquake hazard, diurnal range temperature, dew point temperature, min temperature, max temperature, precipitation rainfall, relative humidity).

5. ANOVA

ANOVA is a technique that, in its simplest form, provides a statistical test of whether or not the population means of a number of samples are equal. It is usually employed to analyze categorical independent variables (herein, deterioration factors) for their effect on the dependent variable (superstructure condition). In the present study, all numerical variables were transformed to categorical variables by utilizing their distributions to form meaningful groups of values. To assess the importance of the differences found for each variable’s groups, ANOVA results were visualized using multiple comparisons Tukey-Kramer method [13]. Certain cases were selected to be presented herein that show important patterns found among groups of the variables studied.

The multiple comparisons presented in Figure 5 show the effect of each variable’s groups to superstructure condition. For each group of values, an average value of the superstructure condition is represented by a circle. The magnitude of the error of the average estimate is indicated with a line in the center of each circle; actually, dots indicate small errors, while lines larger ones. Furthermore, increased difference between a variable’s group means indicate the higher importance of the variable to superstructure deterioration.

Figure 5(a) demonstrates the high importance of year of construction or rehabilitation in the structural condition of bridge superstructures. It is also clear from the same figure that differences in superstructure condition between rehabilitated bridges (upper part of Figure 5(a)) and non-rehabilitated bridges (lower part of Figure 5(a)) exist. On the other hand, as regards Average Daily Traffic, only minor differences are observed between group means (Figure 5(d)).

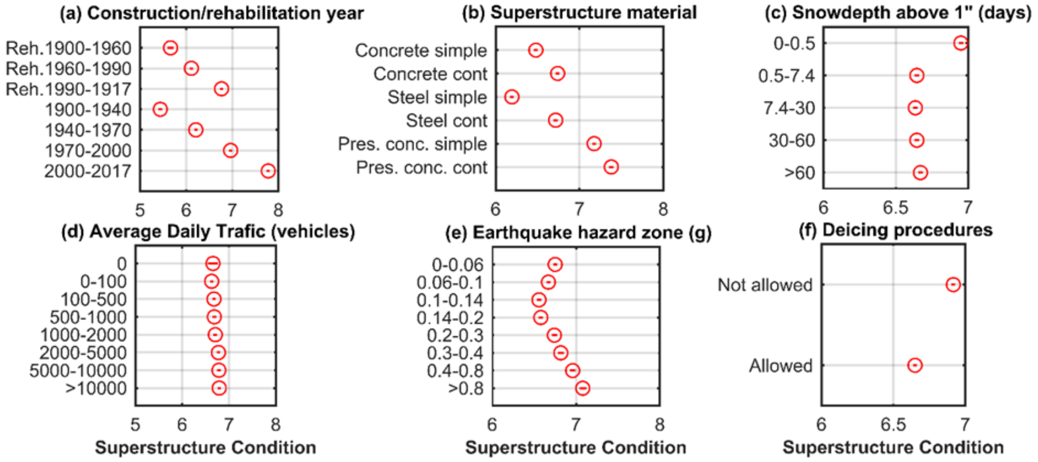


Figure 5. ANOVA results for selected bridge deterioration factors displayed using multiple comparisons.

The structural materials utilized in superstructures also appear to have increased differences between their group means (Figure 5(b)). Simple-span superstructures made of structural steel seem to be in the worst condition, while prestressed concrete superstructures with continuous span are on average in the best condition.

Regarding the earthquake hazard variable, Figure 5(e) shows that up to a certain group (PGA 0.14-0.2g), bridges tend to have decreasing mean condition for increasing PGA level. This effect is reversed for the means of the higher PGA groups, which could be attributed to the more demanding design standards for bridges built to withstand higher seismic actions in locations with increased earthquake hazard.

Figure 5(f) shows that, as expected, the use of deicing salt negatively affects the mean condition of superstructures. According to Figure 5(c), the days of snow depth above 1 inch do not have an effect on the mean superstructure condition, with the exception of the first group (0-0.5 days). However, as can be seen in Figure 3, the first group roughly coincides with the non-deicing region, where the use of deicing salts is not allowed, which explains the better mean superstructure condition for this group. As regards the other groups exhibiting practically the same mean condition, it seems that superstructures are affected by the presence of deicing salts, irrespective of the snow volume on the deck surface.

6. Regression analysis

Regression analysis is a statistical process for modelling and analyzing the relationship of a dependent variable with one or more independent variables. It is commonly used for prediction and forecasting, but it has also been utilized for achieving a better understanding of the relative importance of each independent variable in modelling the dependent variable.

In the negative binomial regression analysis performed herein, the initial number of variables studied were reduced based on the obtained results from correlation analysis and ANOVA. The independent variables included in the analysis are shown in Table I. For these variables, an additive, generalized linear model fit was calculated using MASS library in R [14]. An initial regression was performed to fit a model using all independent variables. Then, a stepwise regression process was utilized, according to which independent variables were added (forward regression) or removed (backward regression) and the so-called Akaike Information Criterion was employed to indicate whether a better model was achieved. By comparing the results of successive regression models, conclusions on omitting unnecessary variables were reached.

Table I: Regression analysis results for superstructure condition rating.

Variable		**Coefficient Estimate**
-		Intercept = -5.3E+00
Length (m)		C1 = -4.8E-05
Maximum span (m)		omitted
Deck width (m)		C2 = 7.1E-04
Year constructed (date/year)		C3 = 3.6E-03
Detour length (km)		C4 = 1.4E-04
Average Daily Traffic - ADT (vehicles)		C5 = 2.7E-08
Truck traffic (% ADT)		omitted
Earthquake hazard - PGA (g)		C6 = 4.9E-02
Precipitation (inches)		C7 = -5.6E-04
Snow depth above 1 inch (days)		C8 = 1.6E-04
Deicing	Not allowed	-
	Allowed	C9 = -2.5E-02
Material	Concrete continuous	-
	Concrete simple	C10 = -9.6E-03
	Prestressed concrete continuous	C10 = 2.1E-02
	Prestresssed concrete simple	C10 = 1.8E-02
	Steel continuous	C10 = 9.8E-04
	Steel simple	C10 = -4.6E-02
Water Underneath	No	-
	Yes	C11 = -7.3E-03

In the regression function obtained, the logarithm of the superstructure condition rating is equated to an intercept term and the added independent variables multiplied by each variable's coefficient:

$$\begin{gathered}\ln\text{(Superstructure Condition)} = \text{Intercept} + C1{*}\text{Length} + C2{*}\text{ Deck width} \\ + C3{*}\text{ Year of construction} + C4{*}\text{Detour Length} + C5{*}\text{ADT} + C6{*}\text{PGA} \\ + C7{*}\text{Precipitation} + C8{*}\text{Snow depth} + C9{*}\text{Deicing} + C10{*}\text{Material} \\ + C11{*}\text{Water underneath} \qquad (1)\end{gathered}$$

The intercept term is a grand average of the dependent variable, while the effect of the various independent variables is indicated by the estimated coefficients provided in Table I. The categorical independent variables included in this table are handled through binary dummy variables (one dummy variable is introduced for each group of a categorical variable). These dummy variables can take only the values of 1 (to activate the coefficient for the specific group) or 0 (to deactivate it). For example, as regards superstructure material, there is no coefficient for 'concrete continuous', thus C10 is deactivated (the dummy variables for all other groups take the value 0), i.e. Eq. (1) is by default calibrated for the particular material. If another material is used, then Eq. (1) needs a 'correction' to shift its result, which is achieved by activating the C10-value (with a dummy variable value equal to 1) of the corresponding group of Table I. Clearly, only one group of a categorical variable and its coefficient value can be active and have a dummy variable value equal to 1 at any time (all other dummy variable values for the remaining groups of the categorical variable are equal to 0 to deactivate the corresponding regression coefficients).

The increase of the value of each independent variable causes either increase or decrease of the value of superstructure condition, depending on the sign of the respective regression coefficient. The regression analysis results reveal the most influencing factor, which is the year of bridge construction, as well as the least influencing ones, which are the bridges' geometric characteristics. The traffic characteristics appear to have a small effect on the superstructure condition. Indeed, the results for ADT are in agreement with the corresponding results obtained with ANOVA in the previous section. The same applies for earthquake hazard, with increase of the PGA value having a positive effect on superstructure condition. Increased annual precipitation and days of snowfall above 1 inch cause a decrease in superstructure condition. The same applies for bridges, which are located in deicing regions or have water underneath. Furthermore, the structural materials used in superstructures appear to have effects similar to the ones observed with ANOVA.

7. Conclusions

In this paper, factors affecting the superstructure condition of bridges were studied using data from existing bridges located in the US. To perform this task, recorded inspection data for more than 600,000 bridges included in the NBI database were utilized. Since the US territory contains a large variety of environmental exposures, the databases of NOAA and USGS were used to introduce additional (non-NBI) variables regarding climate and earthquake hazard. To estimate data values for each bridge location, spatial interpolation methods were implemented. The combined dataset including NBI and non-NBI data was then analysed using data analysis procedures, to determine which variables affect the structural condition of bridges.

The exploratory data analysis performed showed that there are low correlations among the selected NBI variables in contrast to climate variables, which were moderately to highly intercorrelated. ANOVA and multiple comparisons revealed useful patterns, which indicated the effect of each variable to structural condition rating. Moreover, the analysis showed the existence of certain thresholds, after which variables have a different effect to the condition ratings, such as the deicing policy implemented and the days of snow depth above 1 inch: although the deicing region coincides with the region of more than 0.5 days of snowfall above 1 inch, further increase in days of snowfall do not affect superstructure condition rating.

The regression analysis confirmed that superstructure condition is mostly affected by:

1. Year of construction
2. Materials of superstructure
3. Earthquake hazard
4. Deicing practices region
5. Precipitation
6. Water underneath.

Less important factors for the superstructure condition were:

1. Average daily traffic
2. Truck traffic
3. Detour length
4. Geometric characteristics

References

[1] Federal Highway Administration (FHWA) (1995) *Recording and coding guide for the structure inventory and appraisal of the nation's bridges*. Washington D.C.: US Department of Transportation.

[2] Mauch, M. and Madanat, S. (2001) Semiparametric hazard rate models of reinforced concrete bridge deck deterioration. *ASCE Journal of Infrastructure Systems*, 7(2), pp. 49-57.

[3] Chang, M., Maguire, M. and Sun, Y. (2017) Framework for mitigating human bias in selection of explanatory variables for bridge deterioration modeling. *ASCE Journal of Infrastructure Systems*, 23(3), 04017002.

[4] Kim Yail, J. and Yoon, D.K. (2010) Identifying critical sources of bridge deterioration in cold regions through the constructed bridges in North Dakota. ASCE Journal of Bridge Engineering, 15(5), pp. 542-552.

[5] Radovic, M., Ghonima, O. and Schumacher, T. (2017) Data mining of bridge concrete deck parameters in the National Bridge Inventory by two-step cluster analysis. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, 3(2), F4016004.

[6] National Oceanic and Atmospheric Administration (NOAA), www.noaa.gov, accessed 5 March 2017.

[7] United States Geological Survey (USGS), www.usgs.gov, accessed 20 March 2017.

[8] Tukey, J.W. (1977) *Exploratory data analysis*. Reading, Massachusetts, USA: Addison-Wesley Longman, Inc.

[9] Neville, A. (1995) Chloride attack on reinforced concrete: an overview. *Materials and Structures*, 28(1), pp. 63-70.

[10] Federal Highway Administration (FHWA), Road weather management program: https://ops.fhwa.dot.gov/weather/weather_events/snow_ice.htm, accessed 5 February 2017.

[11] Chen, W.-F. and Duan, L. (2014) *Bridge engineering handbook: Seismic Design, 2nd ed*. Boca Raton Florida: CRC Press.

[12] Mair, A. and Fares, A. (2011) Comparison of rainfall interpolation methods in a mountainous region of a tropical island. *Journal of Hydrologic Engineering*, 16(4), pp. 371-383.

[13] Wilcox, R.R. (2009) *Basic statistics (understanding conventional methods)*. Oxford, New York: Oxford University Press.

[14] R Development Core Team (2008) *R: A language and environment for statistical computing*. Vienna, Austria: R Foundation for Statistical Computing.

A Simulation-driven Approach for Measuring Risk and Resilience in the Network of Critical Infrastructures

Stefan Schauer, Thomas Grafenauer, Sandra König
Center for Digital Safety & Security, AIT Austrian Institute of Technology
Lakeside B10a
9020 Klagenfurt, Austria

Stefan Rass
Institute of Applied Informatics, Universität Klagenfurt
Universitätsstrasse 65-67
9020 Klagenfurt, Austria

Abstract

In this article, we present a simulation-based approach for measuring risk and resilience, which combines the assessment of potential threats for individual infrastructures with the estimation of their resilience against those threats. In particular, our approach focuses not only on the individual infrastructures but takes the whole network of critical infrastructures (within a region or an entire state) into account. To achieve that, we explicitly consider the network of critical infrastructures, which is made up by the interdependencies between the individual infrastructures. By applying stochastic models, the cascading effects of an incident within this critical infrastructure network can be simulated. Using a simplified example, we show how the risk and resilience measure can be computed and how the results can be interpreted.

Keywords: risk and resilience measure, critical infrastructure network, cascading effects

1 Introduction

Critical infrastructures (CIs) provide core functionalities for the well-being of society, including the supply with necessary utilities (power, gas or water), communication infrastructures as well as goods and medical care. In recent years, CIs have become an attractive target for attackers, in particular from the cyber domain, and such attacks might cause a limitation of the infrastructures operation or even a complete shutdown (as, for example, the attacks on the Ukrainian power grid in 2015 and 2016 [1], [2]). Furthermore, the constantly growing number of ever more complex connections between the individual CIs increased the degree of mutual dependencies among them. Thus, the interconnected network of CIs, e.g., within a region or a state, has developed into an overall system that is sensitive to disruptions [3]–[6].

Because of these strongly interrelated dependencies, an impairment or even total failure of a critical infrastructure not only affects this infrastructure alone but may also have an impact on a number of other critical infrastructures as well as on the economic and social well-being of the population (cf. for example [7]–[11]). Therefore, an in-depth risk and resilience management has become a core duty of critical infrastructure operators to be aware of the effects and consequences of incidents potentially threatening the infrastructure. Although such systems to assess risk and resilience of a CI are often already used by the operators, it is difficult to take the complex dependencies to other CIs into account and evaluate the cascading effects of an incident on the entire system.

In the course of a national research project called CERBERUS (Cross Sectoral Risk Management for Object Protection of Critical Infrastructures), which was funded by the Austrian Research Promotion Agency (FFG), we developed a simulation-based analysis which considers aspects from risk as well as resilience management. For this purpose, stochastic models (in particular Markov chains) are used, which describe the potential consequences of interdependencies between different CIs. The effects of a capacity reduction or a total failure of an infrastructure are simulated on the basis of this model over a fixed period of time.

In this article, we want to describe how this simulation-based analysis can be used in practice to evaluate a risk and a resilience level of the individual CIs in a CI network. The main focus is to identify and estimate cascading effects among the CIs, which can manifest due to the interdependencies in the CI network. To achieve that, we combine elements of a static and a dynamic risk analysis with a methodology to compute resilience. All three models are build on the same stochastic model for describing the operational states of a CI and how these can change due to external influences. In more detail, we will provide a short overview in the following Section 2 on how we use the concept of CI interdependency graphs in our approach. Section 3 describes how the static and dynamic risk model is defined and how the simulation is building on these models. The resilience model is sketched in Section 4 and Section 5 brings both models together in an example, showing the results of the risk and resilience computation. Interpretation and additional thoughts on the results are given in Section 0.

2 CI Interdependency Graph

The approach developed in the course of the CERBERUS project builds upon the concept of the CI interdependency graph. The modelling of interdependencies among critical infrastructures has been widely discussed in the literature [3]–[6] and therefore this concept is extensively used by several approaches. Particularly when it comes to describing and simulating cascading effects among the critical infrastructures, the CI interdependency graph is used as a basic structure for the simulation and estimation of cascading effects [12]–[16]. The main benefit of such a graph representation is that general graph-theoretic concepts and algorithms can be applied to describe the propagation of the effects of an incident through the network of interrelated critical infrastructures.

In more detail, our approach represents each CI as a node and each dependency between two critical infrastructures as a directed edge. Let's consider a water provider W as critical infrastructure that depends on a power provider P to supply electricity and the transport infrastructure T for the supply with materials and other equipment (cf. **Error! Reference source not found.**). In the infrastructure graph, we can indicate these two dependencies as directed edges from the nodes P and T to the node W. Furthermore, the water provider is an essential supplier for other CIs, e.g., a hospital H and a food supplier F; both require water in their daily business to work properly. This is represented by a directed edge from W to H and F. In this way, an interdependency graph for all the CIs within a region or a state can be built up, indicating a general "supplier / customer" relationships between them.

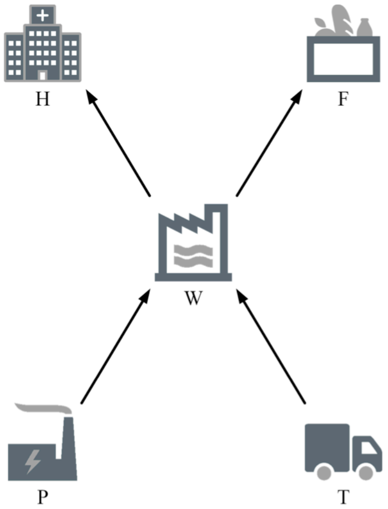


Figure 1 Simple illustration of the CI interdependency model

However, the graph itself does not provide any details on how much the individual infrastructures influence each other. Therefore, the interdependency graph in our approach takes one step further and models the operational state of each CI, i.e., each node can be in one of several different states, since an incident within a critical infrastructure might not always (and immediately) cause its total breakdown. Rather an impairment in the functionality of the power provider P could have a small or large effect on the operational state of the water provider W, depending on how dependent CI W is on the resource or service provided by CI P. Thus, each node has n different operational states k_i, which can be represented by categories $(k_1 \cdots k_n)$ or colors, and each state is connected (via the dependency between the two CIs) with the operational state of its suppliers. Hence, the operational state of a CI may or may not change depending on the operational state of its suppliers.

3 Risk Analysis

The risk model consists of two main components, the static and the dynamic risk model. The static risk model focuses on the basic characteristics within a CI by breaking it down into individual components. In the dynamic risk model, the operational states of a CI and how they can change due to dependencies on other CIs are considered. Risk analysis is then achieved by simulating the effects of an incident on the dependent critical infrastructures, which can lead to a partial or total failure of one or multiple CIs.

3.1 Static Risk Model

The static risk analysis in our approach is based on detailed information about the individual CIs in the network and describes their internal structure and generally uses the principle of a gap analysis. The existing measures and controls, which are already implemented within a CI, are compared with the potential threats and the extent to which the measures affect the respective threat is analyzed. For each control, a maturity level can be specified which describes the effectiveness of the control against a particular threat and thus influences its effects.

In the course of a risk assessment, both the relevant threats and the implemented measures are identified for each infrastructure. In principle, we follow the intuitive rule: the higher the degree of maturity, the lower the damage caused by a hazard. The damage can be expressed in various term, i.e., by an abstract qualitative scale, by the monetary loss directly connected to the effects of the threat, or by using several different indicators to assess the effects in multiple domains. In the context of CIs, the monetary approach is not the best one since a failure within a CI will often effects on the society itself, which can’t be measured in monetary terms. For the remainder of the article, we will use an abstract scale of ordinal numbers based on the operational state of the CI to describe the impact of a threat. This scale will range from 1 to 3, where “1” means that there is no problem and the CI is fully operational, “2” indicates that there are some problems but the CI is still working to some extent and “3” represents a complete breakdown of the CI.

3.2 Dynamic Risk Model

The dynamic risk analysis builds upon the CI interdependency graph described in Section 2 above, i.e., on the relations between the CIs, and on the operational state of each individual infrastructure (cf. Figure 2). A CI can be in one of n different operational states, given as a category k that we hereafter synonymously associate with the CI’s state, and the CI might change from one state to another based on the operational states of its suppliers. In order to model a state change, each edge between two CIs is extended by a multinomial distributed random variable [17], which describes the probability that, e.g., the water provider W goes from state k_i to k_j based on the current state of the power provider P. This can be understood as a (generalized) Markov chain, similarly to the approach described in [15], [16].

To describe this in a more formal way (cf. also [18]), we model each individual CI as a bipartite weighted graph, i.e., each node in the CI interdependency graph also has a graph structure (as displayed in Figure 2). This sub-graph representing an individual CI consists of two sets of nodes, i.e., one set V_1 representing the combination of all possible operational states for all of the CI's supplier nodes, and one set V_2 representing the different possible states which the CI itself can be in. Looking at our running example, each CI can be in one of three different operational statuses, ranging from "1" (fully operational) to "3" (complete breakdown). Thus, V_2 consists of $n = 3$ nodes in our example and V_1 consists of a multiple of three nodes based on the number of suppliers for the CI (e.g., with two suppliers, V_2 would consist of six nodes). In this sub-graph, the edges run from V_1 to V_2; each edge has a weight p_{ij} indicating the probability that the CI changes to the state $v_j \in V_2$ given that one of its suppliers is in state $v_i \in V_1$. These probabilities can then be arranged in matrix form, i.e., as a transition matrix. Hence, these weighted edges formally described the fact that a change in the operational state of one CI is based on the operational state of its suppliers.

Moreover, since there might me several suppliers for one CI, the set V_1 takes all possible operational states of all the suppliers into account. Accordingly, there will be in general more than one edge leading to one of the nodes in V_2 (i.e., to one of the CIs operational states). In this case, there might be several options in which operational state a CI could end up in. Therefore, we are using a maximum approach, i.e., after evaluating the probabilities given by the edges from V_1 to V_2, we take the worst case state (i.e., the highest number) as the new operational state of the CI.

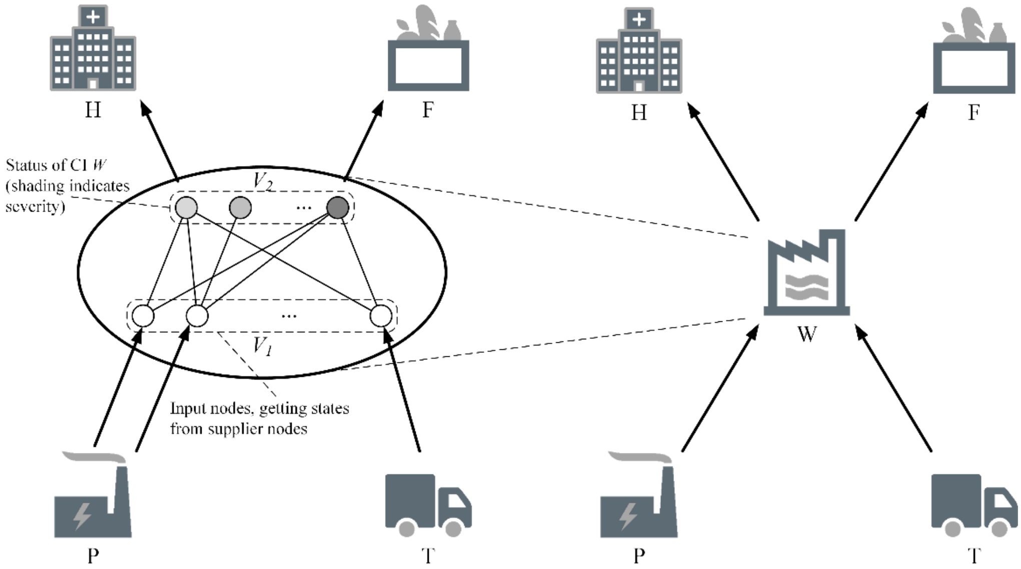


Figure 2 Description of the internal graph model for a specific CI

Referring to our scenario, the water provider W has two suppliers it depends on (cf. Figure 2). In case the road to the water power plant is blocked and thus the transportation infrastructure breaks down (i.e., it changes to state "3"), the immediate effect on the water provider W might be minimal. We assume that W does not need constant supply for its daily business and can still operate at full capacity for some time even if the transportation infrastructure T is blocked. Thus, the state change in T

from “1” to “3” will not change the state of W. In terms of the sub-graph representing the water provider W, there is an edge from one node $t_2 \in V_1$ (which represents T being in state “3”) leading to $w_0 \in V_2$ (which represents W being in state “1”) with the weight 1. Further, if the power provider P suffers severe damage and has to shut down (i.e., changes its operational state to “3”), the water provider might be seriously affected. Hence, there is an edge from one node $p_2 \in V_1$ (which represents P being in state “3”) leading to $w_2 \in V_2$ with weight 1. Thus, the water provider switches to state “3”, since there is no emergency power supply in our example. Further, this also represents the worst case for the water provider and thus W will go into state “3”.

3.3 Dynamic Simulation Model

Based on the specification of the dynamic risk model in the previous section, simulations are used to describe the evolution of the overall CI network in case one or more CIs are exposed to a threat. This is achieved by implementing and evaluating the stochastic model based on a specific incident initiated in the beginning by the user and by performing a large number of simulation runs. Based on that, the operational states of the CIs in the network change according to their interdependencies which will lead to an overall finite state at the end of a simulation run. When looking at the total number of runs, the distribution over these final operational states for each CI can be estimated, providing an overview on the cascading effects of the incident within the entire CI network.

Additionally, to achieve a more realistic impression of the CI network’s evolution, we further extend the graph model and the Markov chain model described above with a time-dependent aspect, thus allowing the chain to be *inhomogeneous*. Therefore, we allow the weights of the edges between V_1 and V_2, i.e., the probabilities for a change of the operational state, to change during the runtime of the simulation. Thus, we can also model the case that a threat becomes more sever the longer it affects a CI. For example, taking a complete outage of the power supplier P, the water provider might still be able to fulfill its services for some time, because an emergency power generator is present. However, when the capacity of the emergency generator is exhausted, the water provider will become seriously affected and also have to shut down due to the lack of power supply.

Technically, this time-dependency of the state changes can be realized using individual transition matrices for the different time periods. In the course of the CERBERUS project, we are looking at three time frames, i.e. short, medium and long term. These time frames can be defined individually for each CI, since short, medium and long term have different meanings for different sectors. As briefly mentioned above, the blocking of the transportation infrastructure could be tolerated for much longer time than the lack of a power supply.

Practically, the probabilities for each of the individual transition matrices have to be defined. Accordingly, the more operational states are used and the more fine grained the time frames are defined, the more values need to be gathered, most likely from experts. Hence, a trade-off is required between the accuracy and efficiency when using the model in a real-life environment. In the CERBERUS project, we found that using three operational states and three time frames represents a practically feasible tradeoff.

4 Resilience Model

For measuring resilience, we are also relying on the CI interdependency graph as a basis and understand the term as the ability to "resist" the consequences of an incident. Therefore, [19] defines the resilience for a CI W as

$$R(W) = \sum_{s=1}^{N} \omega_s \cdot \left(P_{s,W} - E\left[I_{s,W}\right]\right) \tag{1}$$

with the sum running over all considered scenarios s, ω_s being the probability of the respective scenario to occur, $E\left[I_{s,W}\right]$ denoting the expected impact for the CI W and $P_{s,W}$ indicating the preparedness of CI W against the scenario s. The resulting number $R(W)$ representing the resilience can either be positive, which indicates a good robustness or negative, which indicates that additional measures need to be taken. It has to be noted that the sum in (1) is a weighted average over all considered scenarios. Hence, if the resilience is negative, the preparedness against the individual threat scenarios will contribute to a different amount to this value. Accordingly, when measures to increase the preparedness are considered, they will not equally help to increase the resilience measure.

For estimating the parameters required to compute the resilience measure, detailed information about the CI and its dependencies is used (cf. also [19]); such information is already at hand from the risk analysis described in the previous sections. In detail, the static risk model described in the previous Section 3.1 provides a list of the controls and measures, which are implemented in a CI. Based on the maturity level that is assigned to each of the measures, the preparedness level $P_{s,W}$ can be estimated, i.e., the higher the maturity level, the better the preparedness. Further, the impact is coming directly from the dynamic model and the simulation approach described in Section 3.2 and Section 3.3, respectively. More precisely, the simulation describes the operational state of all CIs in the network when a specific threat scenario affects one (or more) CIs in the network. Since the simulation is based on a stochastic process, we take the expected impact $E\left[I_{s,W}\right]$ as each impact category (from "1" to "3") weighted with the respective probability coming out of the simulation process. Finally, the list of the threat scenarios that need to be considered can come from a classical risk analysis. As part of this, also the probabilities of a scenario to occur are estimated by experts within the CIs.

5 Example

5.1 Example Setup

For our example, we are looking at a water provider at the core of a CI network consisting of infrastructures from several different sectors (this example is based on previous work in [18], an illustration is given in FIG). Besides a power plant, a hospital and a (generic) food supplier, we model the electric power grid, the telecommunication network and the gas distribution network as single node for reasons of simplicity. Additionally, we also consider an emergency gas supply, i.e., a node which can provide gas for a limited amount of time in case the gas distribution network encounters any problems. Furthermore, we also look into the water provider and model its internal components: a mountain spring, a river spring, a water well, a river pump, a water well pump, a water reservoir, and a water facility. Thereby, we want to show that our simulation approach can handle the external view on CIs as well as their complex internal structure.

In the example, we look at three different scenarios. These scenarios mark the initial events of the simulation (but could also take place a certain point in time later on), have a specific duration and affect one or more of the CIs in the network. The first scenario is a classical natural threat, i.e., an extreme weather condition, which lasts for three hours and affects the electrical grid. The second scenario describes a technical threat, i.e., an accident with hazardous goods, which lasts for two hours and affects the natural gas network and the hospital. The third scenario is a cyber threat, i.e., an attack by hackers on the Supervisory Control and Data Acquisition (SCADA) systems controlling the pumps within the water provider. This attack causes the pumps to stop their operation immediately at the beginning of the simulation.

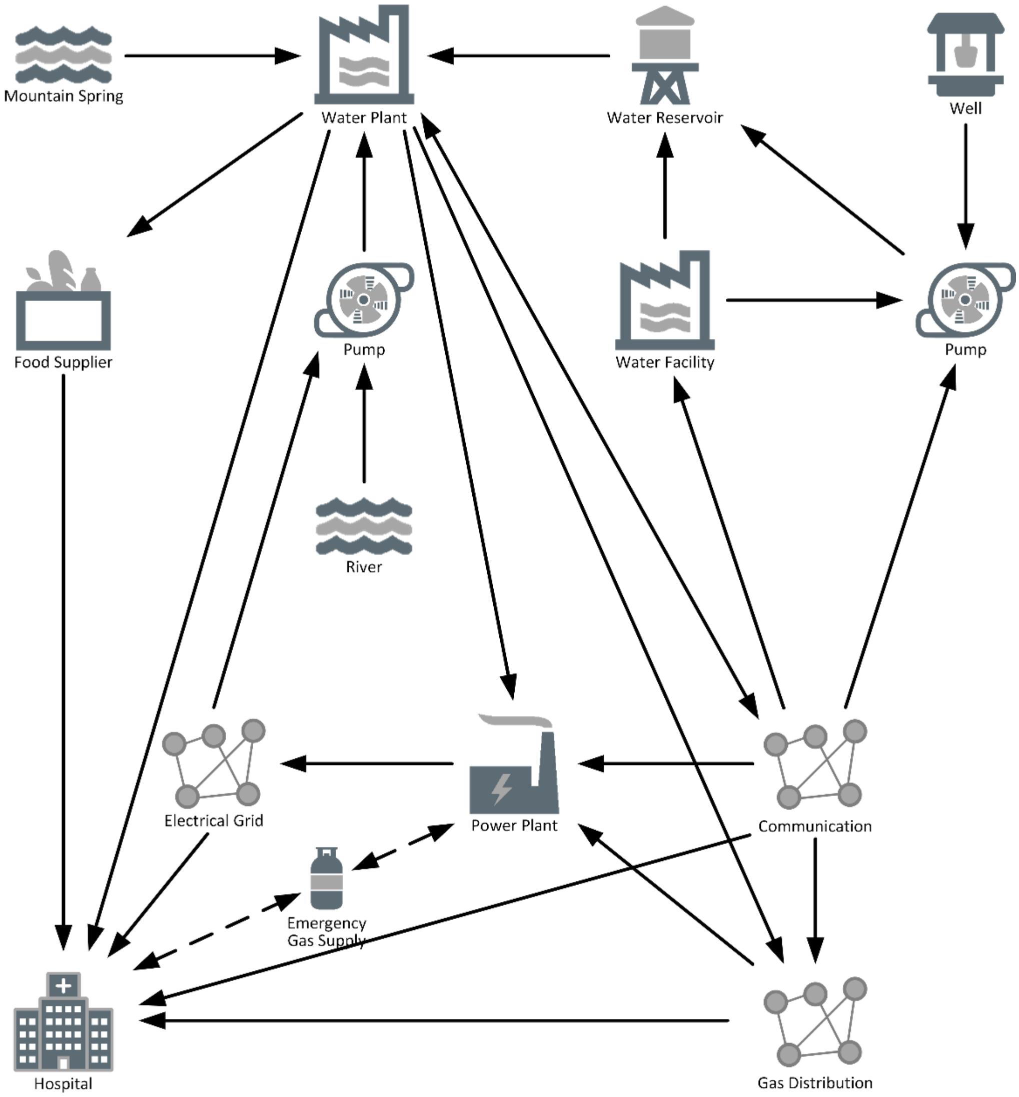


Figure 3 Illustration of the example setup

5.2 Simulation

As a main output, the simulation computes the final operational states of all CIs within the network and also keeps track of the intermediate changes in the network. Therefore, a large number of simulation runs (the number can be chosen by the user) is carried out and the statistics are created for all runs. In this way, the user obtains a distribution over how often a CI ended in one of the three operational states. Further, the simulation also provides a percentage of the intermediate state changes, i.e., the numbers how often the state of one CI changes from “1” to “2”, from “2” to “3” and from “1” to “3”. In this connection, the results also show the most common trigger for a state change, i.e., for each CI *X* it shows which other CI *Y* that CI *X* is directly depending on caused the operational state of CI *X* to change. This information can be used to identify CIs in the network, which cause a lot of problems at other CIs due to their interdependence. Additionally, the simulation also keeps track of the results of each individual run. Hence, a chronological record of each CI’s operational state changes can be generated, which indicates at which point in time a CI switched to a more critical state. Furthermore, it is also recorded which CI triggered a state change in another critical infrastructure in each individual run, too.

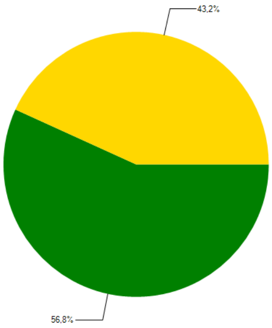


Figure 4 Distribution of the final states for the water plant after all simulations

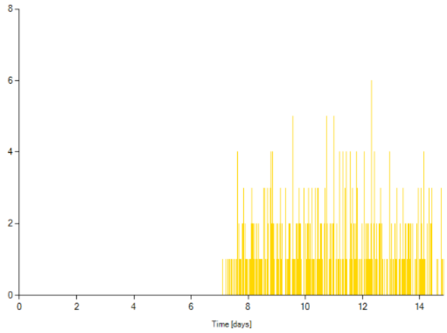


Figure 5 Number and time when the water plant was in final state "2"

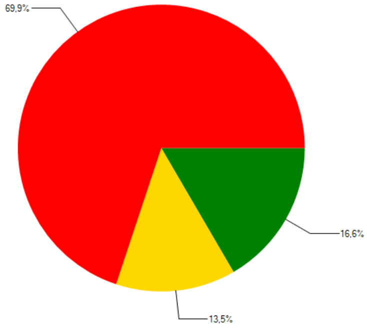


Figure 6 Distribution of the final states for the hospital after all simulations

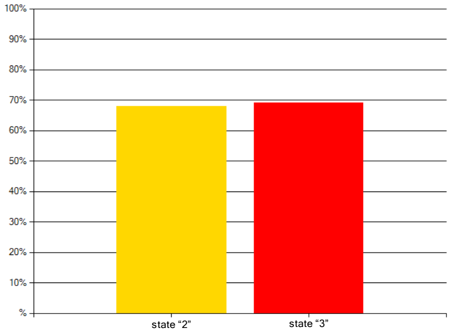


Figure 7 Percentage of state change for the hospital

With regards to the three scenarios defined in the previous section, we performed 1000 simulation runs and will focus only on the average outcomes from all of those runs (and not look at individual runs) since those results will be relevant to compute the risk and resilience for individual CIs. Further, we will only focus on three CIs in the overall network, i.e., the water provider, the food supplier and the hospital, to provide examples of how the risk and resilience can be computed for these three infrastructures. Table 1 presents the percentages of the final operational states for the three CIs at the end of the simulations. From that, we can already see that for all three scenarios, the water plant never reaches a complete breakdown (state "3"), whereas the hospital will have a high chance to end up in this most critical state.

Table 1 Simulation output for the three scenarios

	Scenario 1: Weather			Scenario 2: Accident			Scenario 3: Cyber Attack		
	Operational State			Operational State			Operational State		
	1	2	3	1	2	3	1	2	3
Water Plant	56,8%	43,2%	0,0%	19,1%	80,9%	0,0%	0,0%	100%	0,0%
Hospital	16,6%	13,5%	69,9%	2,5%	11,8%	85,7%	1,7%	8,1%	90,2%
Food Supply	63,2%	24,6%	12,2%	33,2%	45,2%	21,6%	16,7%	59,1%	24,2%

To compute the risk for each CI under each of the scenarios, we are relying on the classical formula *Risk = Probability × Impact*. In this context, we use the operational state as an abstract notion of impact and take the weighted sum over all three states (which corresponds to the Expected Impact $E[I_{s,W}]$ from eq. (1) above). The likelihood for each scenario is usually estimated by experts or taken from historical data. For our small example, we make some guesses and thus a risk value for the scenarios as given in Table 2.

Table 2 Risk values for each CI and for the respective scenario

	Scenario 1: Weather			Scenario 2: Accident			Scenario 3: Cyber Attack		
	Prob.	**Imp.**	**Risk**	**Prob.**	**Imp.**	**Risk**	**Prob.**	**Imp.**	**Risk**
Water Plant	0,33	1,43	**0,47**	0,20	1,81	**0,36**	0,15	2,00	**0,30**
Hospital	0,33	2,53	**0,84**	0,20	2,83	**0,57**	0,15	2,89	**0,43**
Food Supply	0,33	1,49	**0,49**	0,20	1,88	**0,38**	0,15	2,08	**0,31**

Looking at the resilience, we take the formula given in eq. (1) to compute the values for each of the three CIs. The only value missing is the preparedness of each individual CI against each of the scenarios. As already mentioned in Section 3.1 above, the preparedness can be derived from the maturity of security measures or controls already implemented by the CI. Since there will be, in general, a number of different controls at various maturity levels, we will have to take an average over these levels; for reasons of simplicity, we chose integers as preparedness levels. In detail, we estimated the water plant to be very prepared ("3") for scenario 1 but hardly prepared ("1") for scenarios 2 and 3. The hospital is rather well prepared ("2") for scenarios 1 and 2 but hardly prepared for scenario 3 and the food supplier is hardly prepared for all three scenarios. Thus, we obtain the results given in Table 3 below.

Table 3 Resilience values for the three CIs

	Water Plant	Hospital	Food Supply
Resilience	0,21	- 0,63	- 0,50

6 Interpretation of Results

When looking at the risk values given in Table 2, we can directly see that they are no longer expressed in the same abstract categories as the impact (i.e., categories “1” to “3”). More precisely, values can be between 0 and 3, although risk values around or larger than 1,5 already represent high impact events which are highly likely to occur. Therefore, a risk scale needs to be defined, either for each CI individually or a general one for all CIs in the network. For example, a three tier scale with categories “low”, “medium” and “high” could be defined, where values up to 0,66 are considered as a “low” risk, values up to 1,5 are considered as “medium” risk and risk values starting from 1,5 and above are treated as “high” risks. In this case, almost all risk values from our example would be in the “low” category (except for the hospital in scenario 1). Since we just guessed the probabilities for this small example, a deeper inspection might show that, e.g., a cyber attack is much more likely to happen which could bring risk values in the “medium” category. This already indicates the importance of choosing adequate values for the probability of a scenario but also of defining suitable risk categories to fit a CI’s requirements.

Regarding the resilience, there is an interpretation already given in [19] stating that a positive value reflects that the CI is – on average – well prepared against all scenarios considered. Accordingly, a negative value indicates that the maturity of existing measures should be developed or additional measures should be implemented to increase the preparedness of the CI. In our given example, we can see that the water plant has enough measures set in place for the considered scenarios although it is not well prepared for scenarios 2 and 3. This shows that the resilience measure only returns an average score and that there still might be opportunities for improvements in the individual preparedness levels. Additionally, we can see from the hospital that a high potential impact requires a very high preparedness level. This reflects quite well the real-life conditions since if there is a potential threat which could cause a rather big impact, respective security measures need to be implemented to strengthen the infrastructure’s resilience and reduce the risk.

7 Conclusion

In this article, we presented an approach to compute a risk and resilience measure for interdependent CIs. The approach is based on a stochastic model, which allows to simulate the change of the CIs’ operational states over time. In this way, the cascading effects of a single incident happening to one of the CIs can be described and taken into account when evaluating the risk and the resilience of the individual CIs in the overall network. This provides a comprehensive overview on the risk and resilience of an entire CI network and allows to support the decision making process on which security measures should be implemented.

There are still some limitations to the approach, one of them being that the impact and preparedness are treated as abstract categories but the probability of a scenario is given as a decimal number. This makes the results more difficult to interpret; however, simply using categories for the probability does not solve the issue. A second limitation is that the preparedness of a CI needs to be estimated. The concept presented here, i.e., looking at the maturity of security measures already implemented by the CI, marks a good starting point but retrieving the information on the maturity level and combining these levels into one value is still an issue. Thus, we are looking to solutions towards these limitations and in our future research.

8 Acknowledgements

This work was conducted in context of the project "Cross Sectoral Risk Management for Object Protection of Critical Infrastructures (CERBERUS)", supported by the Austrian Research Promotion Agency under grant no. 854766.

9 References

[1] E-ISAC, "Analysis of the Cyber Attack on the Ukrainian Power Grid," Washington, USA, 2016.

[2] J. Condliffe, "Ukraine's Power Grid Gets Hacked Again, a Worrying Sign for Infrastructure Attacks," 22-Dec-2016. [Online]. Available: https://www.technologyreview.com/s/603262/ukraines-power-grid-gets-hacked-again-a-worrying-sign-for-infrastructure-attacks/. [Accessed: 26-Jul-2017].

[3] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEEE Control Systems*, vol. 21, no. 6, pp. 11–25, 2001.

[4] D. D. Dudenhoeffer, M. R. Permann, and M. Manic, "CIMS: A Framework for Infrastructure Interdependency Modeling and Analysis," in *Proceedings of the 2006 Winter Simulation Conference*, Monterey, USA, 2006, pp. 478–485.

[5] Y. Y. Haimes, "Hierarchical Holographic Modeling," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 11, no. 9, pp. 606–617, 1981.

[6] R. Setola and S. D. Porcellinis, "Critical Infrastructure Dependency Assessment Using the Input-Output Inoperability Model," *IJCIP*, vol. 2, pp. 170–178, 2009.

[7] J. Reichl and M. Schmidthaler, "Blackouts in Österreich (BlackÖ.1) - Endbericht," Linz, Österreich, 2011.

[8] J. Reichl *et al.*, "Blackoutprävention und -intervention - Endbericht," Linz, Österreich, 2015.

[9] Schweizer Bundesbahnen SBB, “Nationaler Stromausfall: netzweiter Stromunterbruch auf dem Bahnnetz,” 2005. [Online]. Available: https://www.sbb.ch/de/meta/news.html/2005/6/26822. [Accessed: 05-Apr-2018].

[10] H. Pidd, “India blackouts leave 700 million without power,” *The Guardian*, 2012. [Online]. Available: https://www.theguardian.com/world/2012/jul/31/india-blackout-electricity-power-cuts. [Accessed: 21-Mar-2018].

[11] S. C. Srivasta, A. Velayutham, K. K. Agrawal, and A. S. Bakshi, “Report of the Enquiry Committee on Grid Disturbance in Northern Region on 30th July 2012 and in Norther, Eastern and Noth-Eastern Region on 31st July 2012,” Ministry of Power, Government of India, New Dehli, India, 2012.

[12] T. J. Gordon and H. Hayward, “Initial experiments with the cross impact matrix method of forecasting,” *Futures*, vol. 1, no. 2, pp. 100–116, 1968.

[13] M. Turoff, “An alternative approach to cross impact analysis,” *Technological Forecasting and Social Change*, vol. 3, pp. 309–339, 1971.

[14] Z. Wang, A. Scaglione, and R. J. Thomas, “A Markov-Transition Model for Cascading Failures in Power Grids,” in *2012 45th Hawaii International Conference on System Sciences*, 2012, pp. 2115–2124.

[15] M. Rahnamay-Naeini, Z. Wang, N. Ghani, A. Mammoli, and M. M. Hayat, “Stochastic Analysis of Cascading-Failure Dynamics in Power Grids,” *IEEE Transactions on Power Systems*, vol. 29, no. 4, pp. 1767–1779, 2014.

[16] M. Rahnamay-Naeini and M. M. Hayat, “Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach,” *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1997–2006, 2016.

[17] S. König and S. Rass, “Stochastic Dependencies Between Critical Infrastructures,” presented at the SECURWARE 2017, The Eleventh International Conference on Emerging Security Information, Systems and Technologies, Rome, Italy, 2017, pp. 106–110.

[18] T. Grafenauer, S. König, S. Rass, and S. Schauer, “A Simulation Tool for Cascading Effects in Interdependent Critical Infrastructures,” in *ARES 2018 Proceedings of the 13th International Conference on Availability, Reliability and Security*, Hamburg, Germany, 2018, pp. 1–8.

[19] S. König, T. Schaberreiter, S. Rass, and S. Schauer, “A Measure for Resilience of Critical Infrastructures,” in *Critical Information Infrastructures Security*, Kaunas, Lithuania, 2019, pp. 55–71.

Refining Stochastic Models of Critical Infrastructures by Observation

Stefan Rass

Institute of Applied Informatics, Universität Klagenfurt

Universitätsstrasse 65-67

9020, Klagenfurt, Austria

Stefan Schauer

Center for Digital Safety & Security, AIT Austrian Institute of Technology

Lakeside B10a

9020 Klagenfurt, Austria

Abstract

The simulation of cascading effects in networks of critical infrastructures (CIs) can be approached in various ways, all of which at some point call for the specification of (numeric) model parameters. Taking stochastic models as one popular class of methods, finding proper settings for the values that determine the stochastic models can be a challenge. In this work, we describe a method of graphical specification of a probability value on a qualitative scale, and how to convert and use the obtained value as a prior for Bayesian statistics. The connection is made to the point of having the initial value specified only as an "initial guess", which can be refined using Bayesian statistics. Eventually, under consistency conditions depending on the application, this amounts to an online learning approach that takes the parameter to convergence towards their true values, based on the user's subjective initial guess, but never challenging a person to give a reliable number for a probabilistic parameter.

Keywords: simulation, cascading effect, risk management, stochastic model, security

1 Introduction

Among the biggest challenges in stochastic models is probability. Scientists often provide people with sophisticated model having beautiful theoretical properties, but left with the highly nontrivial challenge of finding proper values for a set of parameters, many of which are probabilities. What if the person simply does not have these values or cannot reliably estimate them? This work proposes to avoid the issue of pulling numbers “out of the air”, by instead resorting to a purely graphical method to specify probabilities. Probabilistic modelling has the appeal of being easy to define and plausible to use, yet the ease of model specification turns into a difficulty when creating a model instance in many cases. Suppose that the model includes some probability parameter p that “simply” quantifies the likelihood of some event to occur; for example, the impact of an incident on related parts in a system (e.g., a dependent infrastructure). Likewise, we may use a parameter (probability) p to describe the likelihood of a threat along risk analysis, or call p the likelihood for human error to bring the human element into a model. How do we set such values in practice? It is tempting to use them in a model because they are easy to argue and statistics enjoys a solid mathematical fundament, but the practitioner facing the challenge of assigning some reasonable value to the variable p may find this to be an almost impossible task to accomplish reliably. In many cases, the setting of such parameters thus resorts to choices on qualitative scales, say, defining the probability just to be “low” or “high”, with the meaning of these values remaining vague or defined by representative standard values specified elsewhere. In many practical cases when people try to *apply* or *use* (not define or invent) stochastic models, the choice of probability parameters is a matter of asking experts for numbers that they simply do not have. This can practically limit the applicability of such models despite any theoretical beauty.

Statistics has lots to offer to people seeking to estimate parameters of stochastic models, since the whole theory of point- and interval estimation is dedicated to the problem of finding values or ranges of values for unknown quantities. Common to most of these techniques is their use of empirical data to compute the estimators. In risk management, and particularly in the context of critical infrastructures (CIs), the situation is just not satisfying the assumptions: data is scarce, and we cannot expect having hundreds of data samples from past incidents in a critical infrastructure (simply because the CI would not have survived the necessary lot of incidents to gather enough data for a statistically reliable estimation).

Instead, we need to come up with a reasonable initial guess for the probabilistic parameters and look for a way to refine that value upon continuous experience. Bayesian estimation thus appears as a reasonable way to go, and this work describes a very straightforward and easy to implement version of such a Bayesian estimation approach, where we explicitly exploit the absence of much prior knowledge as an advantage. Indeed, if there is not too much robust prior knowledge about how a probability parameter should be set numerically, this also means that any choice is as good as the other. While it would not make sense to step forward by just picking parameter values at random, the Bayesian method is much more elegant in letting us choose a prior *distribution* to our own convenience, and – realistically reflecting the uncertainty of the person instantiating the model – leaving the parameter p actually unspecified in the beginning. The actual value for p is then obtained from the prior distribution in first place, and iteratively refined by bringing in experience about the model performance to continuously refine it towards an accurate setting for the real model.

To the end of using that method for model parameterization, we thus have to devise (i) a method to pick a reasonable initial guess for a parameter p (as described in Section 3), and (ii) describe a method to define that guess, which assures that we will eventually end up with the correct value for p over the long run (as covered in Section 4).

As a running example, we will pick a specific model to describe critical infrastructure dependencies, to study cascading effects by simulation. Our choice of the CERBERUS model [1] is arbitrary here, and can be replaced by any other stochastic model based on Markov chains, percolation theory, or others. The palette is rich, and we refer the reader to [2]–[11] for models to which our work may offer an aid to get a practical instance, meaning concrete numeric settings, for the involved probability parameters.

2 The CERBERUS Risk Simulation Model

Consider a network of interdependent critical infrastructures that we represent as a directed graph $G = (V, E)$ with edges $A \to B$ meaning that CI B somehow depends on CI A. For example, A could provide energy, water, food, transport, etc. for B. To all infrastructures in the (node) set V, we assign one out of k possible operational states, reflecting their degree of "health". Typically, this state ranges from "fully functional" (state 1) to "outage" (state k), with intermediate states from 2 to $k - 1$ corresponding to ascending limitations in a CI's service(s). The dependency of a CI B on one or more of its providers may be of arbitrary form and dynamic. For example, a CI may have providers that it vitally depends on, or whose service can be substituted for a limited period of time (e.g., emergency power generators can cover a power outage for some time, until they run out of fuel). Other dynamics of dependency may involve the kind of service more explicitly, say, if CI B relies on online-services of A (e.g., an outsourced data center) in order to coordinate the shipping of goods from another provider C to B.

Commonly, authors distinguish the type of dependency here, dividing it into physical dependencies (e.g., supply with physical utilities), cyber-dependencies (e.g., communication and data exchange), geographic dependency (often physical proximity or reachability), and others (cf. [6], [12]–[15]), including temporal dependencies (that are outside our scope here since we look for the setting of probability parameters).

To study cascading effects in such models, we thus need to describe what happens to an infrastructure if its providers fail. While there is lots of work on understanding dependencies (see [16] for a considerable collection of respective references), quantitative studies on how to describe the parameter value for some stochastic model are rare (not so the models themselves; see the references in the introduction). In this context, we want to highlight the work in [16], where an empirical study on how strong the impact of several critical infrastructures may be on others is provided.

The CERBERUS model uses precisely such information to describe an infrastructure model and cascading effects therein in the following way:

- The behavior of a CI B is described by a bipartite graph, with two layers of nodes (see Figure 1):

  - The top layer has exactly k nodes, one for each operational state in which the CI can be
  - The bottom layer has k nodes per CI A that CI B depends on. That is, each supplier CI A is represented in the graph model as its own set of k nodes, one per operational state of CI A, and every other supplier of B having its own copy of these k input nodes.
- The bipartite inner graph is complete, meaning that there is an edge from each state node of each supplier to the overall state node of CI B. These edges are annotated by probabilities, indicating how likely it is that CI B moves into state j, if infrastructure A is in state ℓ. For each $\ell \in \{1,2,\dots,k\}$, we thus have to specify a probability $p_{\ell j} = \Pr(\text{CI B is put into state } j | \text{ CI } A \text{ is in state } \ell)$. If the change is a (deterministic) fixed consequence, we can put $p_{\ell j} := 1$ to model this.
- Since the edges connect only two nodes at a time (the model is a graph, not a hypergraph), the effects of a supplier on B are independent on what other suppliers do. Moreover, B can be put into distinct operational states upon different of its providers changing their state individually. Intuitively, this reflects the real world quite well, since a problem at provider A_1 may cause only slight stress for CI B, while another (independent) problem at provider A_2 may have a substantial impact on B's functionality. Thus, there is an aggregation function being applied on the states that probabilistically follow from the supplier states, which in the simplest case is just the maximum of all possible states that the suppliers may put B into. For example, if provider A_1's failure puts B into state "normal" (i.e., no immediate effect), but supplier A_2's outage causes severe problems in B, the overall state of B is the worst of the two, set to be "severe problems".

This kind of maximum-aggregation assumes that higher state indices correspond to more severe problems (taking the lowest state as the best). Logically, it corresponds to an OR, since B has troubles if at least one of its critical providers fails. This logic can be changed into an AND by resorting to a minimum-value aggregation, causing the state of B to remain "healthy", unless all of its providers fail. The proper choice per infrastructure is up to the application.

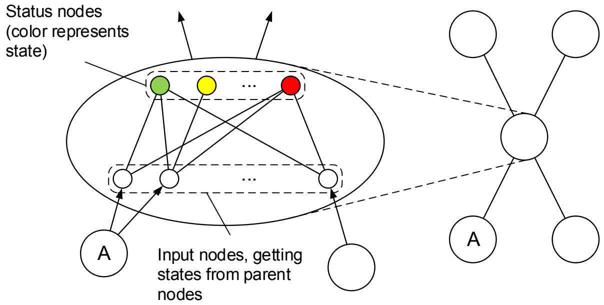

Status nodes (color represents state)
...
...
A
Input nodes, getting states from parent nodes
A

Figure 1 CERBERUS Model (picture adapted from [2])

The CERBERUS model includes this simplification to avoid a combinatorial explosion of parameters that would need specification otherwise. For example, the most powerful description of dependency (that includes the above OR/AND dependencies as trivial special cases) is that of a Bayesian network [17]. This approach is similar to the CERBERUS model, however, requires a worst-case exponential number of parameters specified to describe the dependency as a full-fledged conditional *distribution*. The above reduces that number to "only" polynomially many (exactly $k \cdot n$ conditional probability *values*, if k states are used and the CI depends on n other CIs). Since both, A and B have a common set of possible states, the transition regime can be described as a matrix of the general form:

State of CI B (depending on A's state)

State if CI A	1	2	...	k
1	p^A_{11}	p^A_{12}	...	p^A_{1k}
2	p^A_{21}	p^A_{22}	$\ddots$	p^A_{2k}
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
k	p^A_{k1}	p^A_{k2}	...	p^A_{kk}

The superscript A is here only a reminder that these transitions relate to infrastructure A, and more such matrices would be required to describe the dependency of B on other CIs. The specification is very much like (though not identical) to a transition matrix of a Markov chain, since in each row, there has to be one target state for CI B. Our problem in the following will thus be the specification of these (many) values, using an initial guess and online learning to refine it.

Again, we stress that the choice of this model for illustration is arbitrary, and replaceable by others. The reader feeling more familiar with Markov chains or other models is safe to think along these lines during the remainder of this work. Indeed, we will become more general than the above in considering the estimation of a whole vector of probability values, constrained to form a probability distribution (thus covering the more complex case of Bayesian network specification too).

3 Model Parameterization: Initial Guesses

In absence of empirical data, the best that we can do is resorting to domain expertise, subjective experience and empirical studies as far as they are available (e.g., [16]). However, the problem remains one where experts have to provide (qualitative or better quantitative) values that are usually hard to obtain. One possibility is getting domain experts into discussion to agree on a common assessment (e.g., using systematic methods such as Delphi and/or opinion pooling [18]), which generally means aggregating different assessments into an object (number) that we can start with – an initial guess. Lossless aggregation into a distribution is also possible and has been described for general risk management in [19]; however, this method is out of our scope here, but mentioned as another option to get a prior distribution for Bayesian updating (met later in Section 3.2).

3.1 Graphical Specification of Parameters

To avoid asking people for numbers, graphical ways of specifying probabilities and general risk parameters have been developed. One method aiming to help with the quantification of risk as the product of "likelihood" and "impact" is to let experts draw a "risk rectangle", whose horizontal length reflects the person's (subjective) assessment on a range for the unknown likelihood, and the vertical breadth acts as an interval estimate for the potential impacts; see Figure 2 for an illustration. The area of the rectangle can, but with care, be associated with the usual formula $likelihood\times impact = risk$, where both inputs are ranges reflecting uncertainty. Intuitively, the larger the rectangle is, the more uncertain would the specification be, stressing that even for small areas, the width and height still need consideration in their own meaning of uncertainty (a very thin rectangle has small area, yet may express large uncertainty about one of the coordinates).

As an initial guess for a parameter, such a graphical method may serve as a replacement for a number, since the actual numeric value is easy for a computer to compile from the rectangle's coordinates.

In any case, this is just a heuristic and there is no formal or scientific reason (so far) why any such graphical method should deliver more reliable results than a direct specification. It is as such a matter of usability and convenience to specify values in this way. This potential benefit becomes even more evident if we transfer the idea to the specification of a whole matrix of values, say, a transition matrix of a Markov chain. Why not think of the matrix as a rectangular grid, on which our task is to place masses, proportionally to as how likely it is that state i will take the chain into the target state j. Returning to the CERBERUS model above, we would, for each supplier CI A, have one such matrix to tell B's target state based on A's current state.

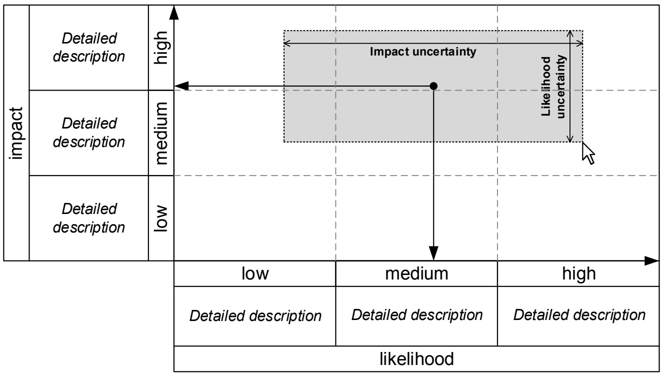
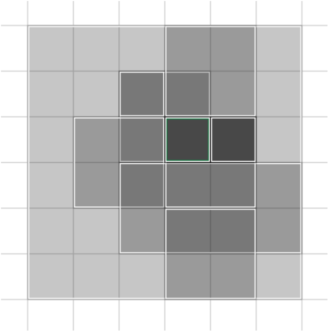


Figure 2 Graphical Risk Specification Method (picture adapted from **[20]**)

The idea is a straightforward extension of the graphical specification from before: assuming that the states are ordered (in ascending or descending levels of criticality), we can go and draw a bunch of rectangles into the grid, which may even overlap, and each of which places some mass onto a cell in the grid, i.e., element in the matrix. The amount of weight being placed is then a matter of how much the rectangle overlaps the respective region. Intuitively, if we draw a rectangle over several cells (horizontally and vertically), we may express something like "any state between i_1 and i_2 may put the dependent CI B into some state between j_1 and j_2" – not becoming too specific on how likely a specific transition is, but only telling what one may think is possible. The more such possibilities are supplied, the more weight accumulates on a cell, and the more likelihood is assigned accordingly. Figure 3 displays the idea, with some example values being assigned.



$$\rightarrow \begin{pmatrix} \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{4} & \frac{1}{4} & \frac{1}{8} \\ \frac{1}{11} & \frac{1}{11} & \frac{3}{11} & \frac{3}{11} & \frac{2}{11} & \frac{1}{11} \\ \frac{1}{15} & \frac{2}{15} & \frac{1}{5} & \frac{4}{15} & \frac{4}{15} & \frac{1}{15} \\ \frac{1}{14} & \frac{1}{7} & \frac{3}{14} & \frac{3}{14} & \frac{3}{14} & \frac{1}{7} \\ \frac{1}{12} & \frac{1}{12} & \frac{1}{6} & \frac{1}{4} & \frac{1}{4} & \frac{1}{6} \\ \frac{1}{8} & \frac{1}{8} & \frac{1}{8} & \frac{1}{4} & \frac{1}{4} & \frac{1}{8} \end{pmatrix}$$

Figure 3 Graphical Specification of a transition matrix

3.2 Prior Distribution for Online Learning

Suppose that we have a set of probabilities $p_1, \dots, p_k$ that jointly form a distribution, i.e., satisfy $p_1 + p_2 + \cdots + p_k = 1$. For the example of the CERBERUS model, given a dependency of CI B on A, such a set would be a matrix as outlined above, or at least a single row in it.

Most likely, the initial guess is inaccurate, subjective, not well founded on empirical data or experience, or suffers from other sources of vagueness. This is most naturally so, since we cannot expect an(y) expert to have precise or objectively reliable figures for likelihoods in a quality better than to the best of her/his knowledge.

It is, however, possible to refine and "correct" these initial guesses in the long run by observing the system, tracking the real state changes, and refine our hypothesis iteratively, knowing that it will converge to the "objective" and hence correct probabilities. The mechanism is Bayesian updating of a properly chosen prior distribution, which makes the whole process even computationally efficient and trivial to implement.

Our choice is the Dirichlet distribution, having $k \geq 2$ parameters $(\alpha_1, \dots, \alpha_k)$ satisfying $\alpha_i > 0$ for all $i = 1, \dots, k$, and the probability density function

$$f_{Dirichlet}(x_1, \dots, x_k | \alpha_1, \dots, \alpha_k) = \frac{\Gamma\left(\sum_{i=1}^{k} \alpha_i\right)}{\prod_{i=1}^{k} \Gamma(\alpha_i)} \prod_{i=1}^{k} x_i^{\alpha_i - 1}.$$

The interesting point for our purpose is the fact that this distribution relates to a vector $\boldsymbol{X} = (X_1, \dots, X_k) \in (0,1)^k$ constrained by $X_1 + \cdots + X_k = 1$, so that it can be used to describe a probability distribution. That is, our sought probability vector, the distribution to be specified, is viewable as a sample of the random vector $\boldsymbol{X}$, whose distribution is Dirichlet with the density as above. Under that perspective, we can equate the needed likelihoods $p_i \coloneqq E(X_i)$ with X_i being the i-th coordinate in $\boldsymbol{X}$.

For the Dirichlet distribution, this expectation is simply

$$E(X_i) = \frac{\alpha_i}{\sum_{i=1}^{k} \alpha_i}$$

Now, suppose that we have an initial guess for the values $p_1, \dots, p_k$; then even without those normalizing to unit sum, we can plainly specify the parameters α_i as $\alpha_i \coloneqq p_i$ to start with, since the denominator in the above expression is nothing else than a normalization, so that the so-instantiated Dirichlet density, encodes our initial guess for the probability parameters by the component-wise expectations.

Remark: The case for a single parameter is treated only slightly different; noting that above, we require at least two values. If there is only a single probability parameter in question, the prior would be the Beta distribution, having the density $f_{Beta}(x|\alpha_1, \alpha_2) \coloneqq f_{Dirichlet}(x, 1 - x|\alpha_1, \alpha_2)$, with the expectation following the same formula as given above. The major (only) difference is that while the Dirichlet distribution describes a set of k probability values, the Beta distribution describes only a single value that is also a probability; in both cases, the last value ($x_2 = 1 - x$ or $x_k = 1 - x_1 - x_2 - \cdots - x_{k-1}$) is fixed by its predecessors (not surprisingly so, since we have the constraint of all these values to sum up to 1).

4 Bayesian Updating

On a level of abstraction, the CERBERUS model is a set of Markov chain instances, where a state transition of a CI triggers another state transition of a dependent CI. Suppose that this switch is observable, i.e., we would note the change in reality, and can relate it to an edge in the model (depicted in Section 2).

Adopting a Bayesian statistics perspective, the observation is nothing else than data sampled from a distribution whose parameters we seek to estimate. More specifically, consider only the i-th row $\boldsymbol{p}_{i,\cdot}$ in a transition matrix $\boldsymbol{P}$, telling us that if the current state is i, then the next possible states $j \in \{1,2,\dots\}$ will occur with probabilities $p_{i1}, p_{i2}, \dots$. This single row is a categorical distribution, and the values in it are exactly the parameters (the distribution is, in a way, not only determined, but actually directly represented by its parameter set). Now, suppose that an observation is made, which tells that out of the current state i, our system has (physically, in reality) moved into the state j. Formally, this is $\boldsymbol{x} = (0,0,\dots,1,0,0,\dots)$, with only the j-th entry being 1, sampled from the aforementioned categorical distribution $\boldsymbol{p}_{i,\cdot}$ (which in turn is just the i-th row in the transition matrix $\boldsymbol{P}$).

More importantly, this view takes the incoming observations as samples from a 0/1-valued random variable. Such a variable is an indicator, and the expectation of an indicator variable is a probability, thus making the approach meaningful to estimate probability parameters.

Now, let us put this to practice: suppose that we observed the event of our system to have undergone a transition from state i into state j. If the Bayesian prior distribution is a Dirichlet (or Beta), with parameters $\alpha_1, \dots, \alpha_k$ (in the case of a single parameter p to be estimated, we would only have α_1 and α_2, with $p = \frac{\alpha_1}{\alpha_1+\alpha_2}$), the Bayesian update of the row $\boldsymbol{p}_{i,\cdot}$ in the transition matrix P, which is described by a prior distribution with parameter vector $(\alpha_1, \dots, \alpha_k)$, proceeds via the assignment

$$\left(\alpha_1, \dots, \alpha_{j-1}, \alpha_j, \alpha_{j+1}, \dots, \alpha_k\right) \leftarrow \left(\alpha_1, \dots, \alpha_{j-1}, \alpha_j + 1, \alpha_{j+1}, \dots, \alpha_k\right),$$

i.e., only the j-th parameter gets increased by 1. What could be simpler? It essentially amounts to counting the occurrences of each transition! Even if several observations are collected in a data vector, say, $\boldsymbol{d} = (n_1, n_2, \dots, n_k)$ with n_1 observed transitions into state 1, another n_2 transitions observed into state n_2, etc., the update to $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_k)$ would simply be $\boldsymbol{\alpha} \leftarrow \boldsymbol{\alpha} + \boldsymbol{d}$.

The current estimate $\hat{p}_j$ of the j-th (not precisely known) probability parameter p_j vector is for each $j = 1,2, \dots, k$ given as

$$\hat{p}_j = E(X_j) = \frac{\alpha_j}{\alpha_1 + \alpha_2 + \cdots + \alpha_k}$$

Now, let us suppose that we started from initial values (guesses) $\alpha_1^*, \dots, \alpha_k^*$. What would happen in the long run? If we observe the transition into the j-th state for N times out of $M \gg N$ cases and let $M \to \infty$, then the estimator $\hat{p}_j$ after a total of M updates is

$$\frac{\alpha_j^* + N}{\left(1 - \alpha_j^* + M - N\right) + \left(\alpha_j^* + N\right)};$$

this is easy to see from the fact that we increase the pseudo-count[1] α_j^* for N times, whilst increasing any of the other parameters for the remaining $M - N$ times (whose totality is collected in the term $1 - \alpha_j^* + M - N$). Overall, since the initial guess does not change, the limit is

$$\frac{\alpha_j^* + N}{(1 - \alpha_j^* + M - N) + (\alpha_j^* + N)} \to \frac{N}{M} = p_j,$$

Since this is merely the fraction of “good cases” among “all cases”, i.e., by definition the sought probability. The key insight here is that this limit does not depend on the initial guess! That is, no matter if we were wrong with our initial parameter choice (and in most cases, we may have been wrong), the long-run updating will asymptotically “correct” our error automatically. Of course, the speed of convergence depends on how far off the inaccuracy of the initial guess put us away from the real value of p_j. The closer our initial guess has been, the earlier we get into a reasonable proximity of the true value p_j.

Let’s also take a closer look at the case of a single parameter: if we don’t have a whole Markov chain, but rather a single parameter that describes an event by a probabilistic value, there is no conceptual change to the above. The respective prior has two parameters (α_1, α_2), which we update to $(\alpha_1 + 1, \alpha_2)$ if the event has been observed, or into $(\alpha_1, \alpha_2 + 1)$ if the event did not occur; both cases assume that the parameter p in question describes the probability of the event’s occurrence (otherwise, the update would be done with the roles of α_1 and α_2 being switched).

[1] A pseudo-count is a fractional count value; this term is technically exact here since we may start from a fractional value α_j, but add 1 upon an observation of the respective transition. Thus, although we do count, the counter’s value remains fractional at all times; hence it is called a pseudo-count.

We refer to [21] for a fully detailed elaboration of this prior idea, which we here generalized. The reference cited treats the topic in the different direction of using the idea for predictive analytics (see [22] for a survey).

4.1 Example for the CERBERUS Model

The application of the above scheme in the CERBERUS model is straightforward, based on what we have: suppose that a history of cascading effects was recently observed in the network of critical infrastructures, or is available from documented cases of incidents or experience. Then, we can consider each part of the chain of events described in the following form: "CI A changed its state from x to y, causing CI B to change its state from u to v". To update our model, we look into the inner model for CI B, which embodies a transition matrix $\boldsymbol{P_A}$ that tells us how likely a change into state v is for CI B, provided that CI A is in state y. Taking that row i of P_A that corresponds to state y, and associating it with its (Bayesian) Dirichlet prior $\boldsymbol{\alpha}_{i,\cdot}^{A} = (\alpha_1, \dots, \alpha_k)$, where k ranges over the possible states of CI B, the update is simply an addition of 1 to the j-th coordinate in the vector α, relating to the state v that CI B turned into. The Bayesian update on this set of transitions is done by that point.

Note that here we did not make any use of the previous states x of CI A or u for CI B. This is due to the fact that the change of state for CI A would be subject to an according update of the inner model for CI A (just as described). The prior state of CI B plays indeed no role here.

5 Conclusion

The above idea is applicable whenever a probabilistic parameter describes an observable event, so that data for a Bayesian update is collectible. A practical issue can indeed be the speed of convergence, since the above argument is nonetheless asymptotic, and the true value is reached only after a hypothetic infinitude of updates. Therefore, we may need to update upon every incoming ticket at the IT administration office, or as often as we can, in practice.

We also stress that the above model does not serve too well as a model of human trust: the updating is in some sense "symmetric" and "self-stabilizing", meaning that (i) the likelihood changes eventually become smaller as more updates come in (self-stabilization), and the likelihoods will update with roughly comparable magnitudes in both directions. The latter is contrary to human subjective changes to trust, since confidence in an event to occur may substantially change upon recent experience and differently in the direction towards zero or towards one. In other words, if the probabilistic parameter is interpreted as a "trust value", say, if we take it as the expectation of some event (that we rely on) to occur, then subjective trust may be lost upon a single incident, but may be regained only over a much longer period of positive experience. On the contrary, the above model would not reflect such asymmetry due to human pessimism. This leads to the advice of applying the above model only for the estimation of parameters that describe *physical* processes, and *not* subjective human factors. The latter are subject to much deeper psychological mechanisms for whose capture the above model may be overly simplistic.

If the parameter in question, however, relates to a physical event that can be observed, then the Bayesian updating as described above offers a computationally efficient and elegant way of online learning parameters in absence of reliable domain expertise to specify a (more) accurate model or prior guess.

6 Acknowledgements

This work was conducted in context of the project “Cross Sectoral Risk Management for Object Protection of Critical Infrastructures (CERBERUS)”, supported by the Austrian Research Promotion Agency under grant no. 854766.

7 References

[1] S. Schauer, S. König, M. Latzenhofer, S. Rass, und T. Grafenauer, „Analyzing Cascading Effects among Critical Infrastructures : The CERBERUS Approach“, 2018.

[2] M. Rahnamay-Naeini und M. M. Hayat, „Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach“, *IEEE Transactions on Smart Grid*, Bd. 7, Nr. 4, S. 1997–2006, Juli 2016.

[3] M. Rahnamay-Naeini, Z. Wang, N. Ghani, A. Mammoli, und M. M. Hayat, „Stochastic Analysis of Cascading-Failure Dynamics in Power Grids“, *IEEE Transactions on Power Systems*, Bd. 29, Nr. 4, S. 1767–1779, Juli 2014.

[4] S. Koenig, S. Schauer, und S. Rass, „A Stochastic Framework for Prediction of Malware Spreading in Heterogeneous Networks“, in *NordSec 2016*, Springer, 2016, S. 67–81.

[5] S. König und S. Rass, „Investigating Stochastic Dependencies Between Critical Infrastructures“, Bd. 11, Nr. 3 & 4, S. 250–258, 2018.

[6] D. D. Dudenhoeffer und M. R. und M. M. Permann, „CIMS: A Framework For Infrastructure Interdependency Modeling And Analysis“, gehalten auf der Proceedings of the 2006 Winter Simulation Conference, 2006.

[7] S. V. Buldyrev, R. Parshani, G. Paul, H. E. Stanley, und S. Havlin, „Catastrophic cascade of failures in interdependent networks“, *Nature*, Bd. 464, S. 1025, Apr. 2010.

[8] Z. Wang, A. Scaglione, und R. J. Thomas, „A Markov-Transition Model for Cascading Failures in Power Grids“, in *2012 45th Hawaii International Conference on System Sciences*, Maui, HI, USA, 2012, S. 2115–2124.

[9] I. Dobson, B. A. Carreras, und D. E. Newman, „A branching process approximation to cascading load-dependent system failure“, in *37th Annual Hawaii International Conference on System Sciences, 2004. Proceedings of the*, Big Island, HI, USA, 2004, S. 10 pp.

[10] I. Dobson, „Estimating the Propagation and Extent of Cascading Line Outages From Utility Data With a Branching Process“, *IEEE Transactions on Power Systems*, Bd. 27, Nr. 4, S. 2146–2155, Nov. 2012.

[11] J. Qi, K. Sun, und S. Mei, „An Interaction Model for Simulation and Mitigation of Cascading Failures“, *IEEE Transactions on Power Systems*, Bd. 30, Nr. 2, S. 804–819, März 2015.

[12] A. Kelic, D. E. Warren, und L. R. Phillips, „Cyber and physical infrastructure interdependencies.“, SAND2008-6192, 945905, Sep. 2008.

[13] S. Rinaldi, J. Peerenboom, und T. Kelly, „Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies“, S. 11–25, 2001.

[14] D. D. Dudenhoeffer und M. und B. R. L. R. Permann, „Decision consequence in complex environments: Visualizing decision impact“, gehalten auf der Proceeding of Sharing Solutions for Emergencies and Hazardous Environments, 2006.

[15] P. Pederson, D. D. Dudenhoeffer, S. Hartley, und M. R. Permann, „Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research“, Jan. 2006.

[16] A. Laugé, J. Hernantes, und J. M. Sarriegi, „Critical infrastructure dependencies: A holistic, dynamic and quantitative approach“, *International Journal of Critical Infrastructure Protection*, Bd. 8, S. 16–23, Jan. 2015.

[17] T. Schaberreiter, P. Bouvry, J. Röning, und D. Khadraoui, „A Bayesian Network Based Critical Infrastructure Risk Model“, in *EVOLVE - A Bridge between Probability, Set Oriented Numerics, and Evolutionary Computation II*, Bd. 175, O. Schütze, C. A. Coello Coello, A.-A. Tantar, E. Tantar, P. Bouvry, P. Del Moral, und P. Legrand, Hrsg. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, S. 207–218.

[18] A. Carvalho und K. Larson, „A Consensual Linear Opinion Pool“, in *Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence*, 2013, S. 2518–2524.

[19] S. Rass, S. Konig, und S. Schauer, „Decisions with Uncertain Consequences-A Total Ordering on Loss-Distributions“, *PLoS ONE*, Bd. 11, Nr. 12, S. e0168583, 2016.

[20] S. Rass, J. Wachter, S. Schauer, und S. König, „Subjektive Risikobewertung – Über Da-tenerhebung und Opinion Pooling“, in *D-A-CH Security 2017*, P. Schartner und A. Baumann, Hrsg. syssec, 2017, S. 225–237.

[21] S. Rass und S. Kurowski, „On Bayesian Trust and Risk Forecasting for Compound Systems“, in *Proceedings of the 7th International Conference on IT Security Incident Management & IT Forensics (IMF)*, 2013, S. 69–82.

[22] P. Kubiak und S. Rass, „An Overview of Data-Driven Techniques for IT-Service-Management“, *IEEE Access*, Bd. 6, S. 63664–63688, 2018.

A Polynomial Chaos method to the analysis of the dynamic behaviour of Vertical Axis Wind Turbine

Abdelkhalak El Hami, Imen Bel Mabrouk
Normandy Univ-INSA-Rouen -LMN
BP 08
76801 Saint Etienne du Rouvray France

Abstract

The services supply disruption of any infrastructure may be due to: systemic (/hardware) failures, procedural (including organizational and human's) failures or a deviation from its normal operation environment. In order to develop robust models to be used in determining the risk of the services supply disruption, one should be able to trace the failure roots as far as the most basic levels. A field of wind-turbines may disrupt its power supply because of a systematic failure of one or more of the basic components of the wind-turbine. This is the case of one of the basic critical components in the wind turbine such as the bevel gear system. The paper proposes an approach to describe the random dynamic behaviour of the bevel gear system of the vertical axis wind-turbine. The polynomial chaos approach is commonly used to treat the random dynamic behaviour of rotating mechanical systems and components.

In the paper, we propose a method for taking into account uncertainties based on the projection on polynomial chaos. The proposed method is used to determine the dynamic response of a bevel gear system with uncertainty associated to power coefficient. We developed a lumped dynamic model with 14 DoFs. Lagrange formalism is used to formulate the governing equation of motion of the model. The simulation results are obtained by the polynomial chaos method for dynamic analysis under uncertainty. The proposed method is an efficient probabilistic tool for uncertainty propagation.

Keywords: uncertainty, bevel gear system, polynomial chaos, Vertical Axis Wind Turbine, performance coefficient.

1. Introduction

The services supply disruption of any infrastructure may be due to: systemic (/hardware) failures, procedural (including organizational and human's) failures or a deviation from its normal operation environment. In order to develop robust models that may be used in determining the services supply disruption/continuity, one should be able to trace the failure roots as far as the most basic levels. A field of wind-turbines may disrupt its power supply because of a systematic failures of one or more of the basic components of the wind-turbine. This is the case of one of the basic critical components in the wind turbine such as the bevel gear system.

The drive train experiences higher failure rates than the other components in the vertical axe wind turbine, [1]. Therefore, studies of dynamic behaviours of the drive train are essential to describe and improve the performance of the system.

Talking into account different sources of uncertainties is a crucial task in accessing the dynamic behaviours of gear systems. Gearbox is identified as the major source of reliability concerns. Nowadays, probabilistic methods have been widely used to solve uncertain dynamic problems of the wind turbine gear system [2-5]. In practice the physical parameters of the aerodynamic model are not exactly known or can be subject to inherent large physical variability. Since the gearbox systems are sensitive to input variations, the uncertainty in the parameters can have a strong effect on the dynamic behaviours of such systems. Subsequently; it is necessary to assess the contribution of the uncertainties into the VAWT dynamic behaviour modelling. Several methods are often proposed in the literature to quantify physical uncertainties in a variety of computational problems. Monte Carlo (MC) simulation is a well-known method in this field [6]. It is based on solving the deterministic problem for randomly chosen parameters values. For reasonable accuracy, a great numbers of samples are usually required. Therefore it is computationally expensive and only used as the last resort. Polynomial Chaos Expansion (PCE) [7] has proven to be a successful probabilistic tool to solve uncertainty quantification problems. The fundamental idea of the Polynomial Chaos method is to establish a separation between the stochastic components of a system response and its deterministic components. The stochastic Galerkin approach, collocation and regression methods are used to solve the polynomial chaos expansion coefficient called stochastic modes in an intrusive and non-intrusive manner while uncertain components are concentrated in the polynomial basis used. The capabilities and efficiency of polynomial chaos approach have been reported in numerous fields, such as uncertainty quantification in computational fluid dynamics and aeronautics [8], in solid mechanics [9], in dynamic systems [10], etc.

The dynamic behaviour of nonlinear system is studied to analyse the robustness and reliability. For that, a dynamic lumped model of one-stage bevel gear system is developed. Three-bladed Darrieus wind turbine are considered with fourteen degree of freedom in the presence of the external aerodynamic torque that is highlighted by an uncertain power coefficient.

2. Dynamic modelling

Fig.1 presents the global model of the one stage bevel gear system in 3D. This model is made up of two blocks. Every block is supported by a flexible bearing. Bending stiffness are donated by $k\psi 1$, $k\Phi 1$ and traction–compression stiffness by $kx1$, $ky1$, $kz1$ for the first block

Stiffness components for the second block are $k\psi 2$, $k\Phi 2$ and $kx2$, $ky2$, $kz2$.

The two shafts between wheel (11) -gear (12) and gear (21) -wheel (22) respectively admit torsional stiffness $k\theta 1$ and $k\theta 2$.

Angular displacements of every wheel are $\theta 11$, $\theta 12$, $\theta 21$ and $\theta 22$. Besides, the linear and angular displacements of the bearings are noted by $x1$, $y1$, $z1$ and $\Phi 1$, $\psi 1$ for the first block, and $x2$, $y2$,$z2$ and $\Phi 2$, $\psi 2$ for the second block.

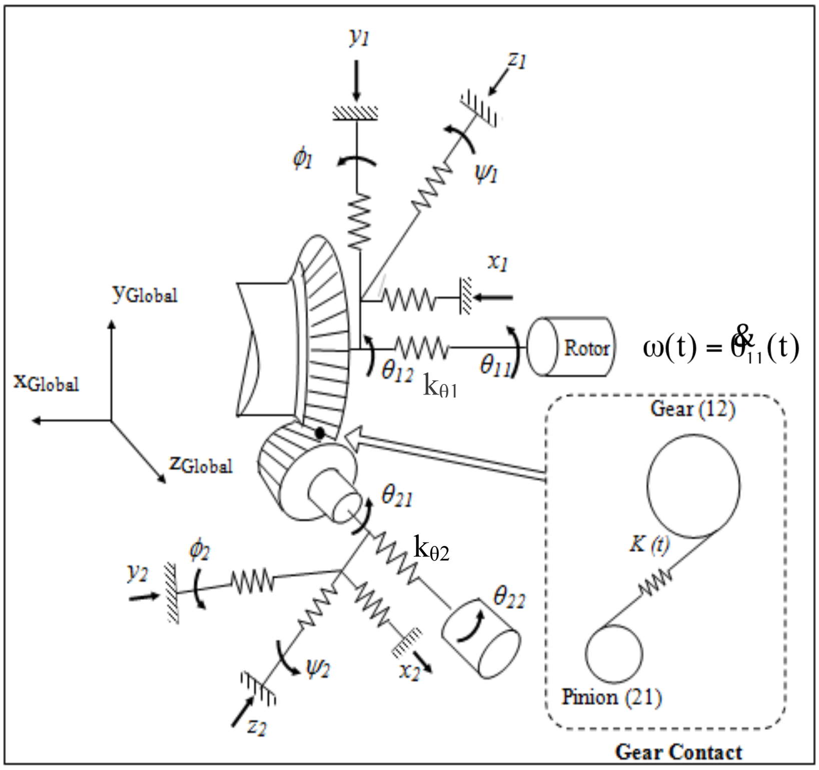


Fig.1. Model of the one stage bevel gear system

The kinematic differential equations governing the system motion established according to Lagrange’s formalism are given by Equation (1).

$$\begin{cases} m_1\ddot{x}_1 + k_{x1}x_1 + k(t)c_1\langle L\rangle\{Q\} = 0 \\ m_1\ddot{y}_1 + k_{y1}y_1 + k(t)c_2\langle L\rangle\{Q\} = 0 \\ m_1\ddot{z}_1 + k_{z1}z_1 + k(t)c_3\langle L\rangle\{Q\} = 0 \\ m_2\ddot{x}_2 + k_{x2}x_2 + k(t)c_4\langle L\rangle\{Q\} = 0 \\ m_2\ddot{y}_2 + k_{y2}y_2 + k(t)c_5\langle L\rangle\{Q\} = 0 \\ m_2\ddot{z}_2 + k_{z2}z_2 + k(t)c_6\langle L\rangle\{Q\} = 0 \\ I_{\phi1}\ddot{\phi}_1 + k_{\phi1}\phi_1 + k(t)c_7\langle L\rangle\{Q\} = 0 \\ I_{\psi1}\ddot{\psi}_1 + k_{\psi1}\psi_1 + k(t)c_8\langle L\rangle\{Q\} = 0 \\ I_{\phi2}\ddot{\phi}_2 + k_{\phi2}\phi_2 + k(t)c_{10}\langle L\rangle\{Q\} = 0 \\ I_{\psi2}\ddot{\psi}_2 + k_{\psi2}\psi_2 + k(t)c_{11}\langle L\rangle\{Q\} = 0 \\ I_{11}\ddot{\theta}_{11} + k_{\theta1}(\theta_{12} - \theta 11) = T_r(t) \\ I_{12}\ddot{\theta}_{12} + k_{\theta1}(\theta_{11} - \theta_{12}) + k(t)c_9\langle L\rangle\{Q\} = 0 \\ I_{21}\ddot{\theta}_{21} + k_{\theta2}(\theta_{22} - \theta_{21}) + k(t)c_{11}\langle L\rangle\{Q\} = 0 \\ I_{22}\ddot{\theta}_{22} + k_{\theta2}(\theta_{21} - \theta_{22}) = T_G(t) \end{cases} \tag{1}$$

m_j is the mass of block (j). I_{11} is the inertia of the rotor, I_{22} is the generator inertia, I_{12} and I_{21} is the inertia of the bevel spur gear 12 and 21. $I_{\Phi i}$ and $I_{\psi i}$ represent the inertia in the y and z-directions respectively. $\langle L\rangle$ is defined by:

$$\langle L\rangle = \langle c_1\ c_2\ c_3\ c_4\ c_5\ c_6\ c_7\ c_8\ c_{10}\ c_{11}\ 0\ c_9\ c_{12}\ 0\rangle \tag{2}$$

The components of tooth deflection are given in Table 1.

{Q(t)} is the vector of the model generalized coordinates, it is given by:

$$\{Q(t)\} = \begin{bmatrix} x_1 & y_1 & z_1 & x_2 & y_2 & z_2 & \phi_1 & \psi_1 & \phi_2 & \psi_2 & \theta_{11} & \theta_{12} & \theta_{21} & \theta_{22} \end{bmatrix}^T \tag{3}$$

3. Numerical results

In this work, the input torque of the bevel gear system is considered with uncertainty according to the performance coefficient (Cp). We use the ODE45 solver of the MATLAB software to calculate the Polynomial Chaos results.

The generalized polynomial chaos theory [article] is proposed to deal with the robust analysis of the dynamic system. The technological and dimensional parameters of the one stage bevel gear system are summarized in Table 3.

Table I: System parameters

Density (42CrMo4)	7860kg/m^3
Teeth number	Z_{12}=45 Z_{21} =18
Pressure angle	$\alpha = 20°$
Teeth module	m=0.004
Contact ratio	ε_α=1.56
Average mesh stiffness(N/m)	K_{moy}=410^8
Bearing stiffness (N/m)	$k_{x1} = k_{y1} = k_{x2} = k_{y2}$ = 2.10^8 k_{z1}= k_{z2}= 4.10^8
Torsional shaft stiffness(N/ m/ rad)	$k_{\theta 1} = k_{\theta 2}$= 310^8

The mean value and the standard deviation of the dynamic component of the angular displacement $\theta_{12}(t)$ are presented in Fig.2.

The mean values and standard deviation of the linear displacement of the second bearing in z- directions are presented in Fig.3.

These figures show that the obtained solutions have random oscillations around the boundary conditions. The standard deviation allows estimating the variation domain of response. One can observe that the dynamic response and the standard deviation have the same order of amplitude.

These results also indicate that small parameter uncertainty might be propagated in the vibration of the bevel gear system and leads to relatively large uncertainties of the dynamic behaviour of the VAWT geared transmission system.

It can be understood from the above discussion that the Polynomial Chaos method is an efficient probabilistic tool for uncertainty propagation.

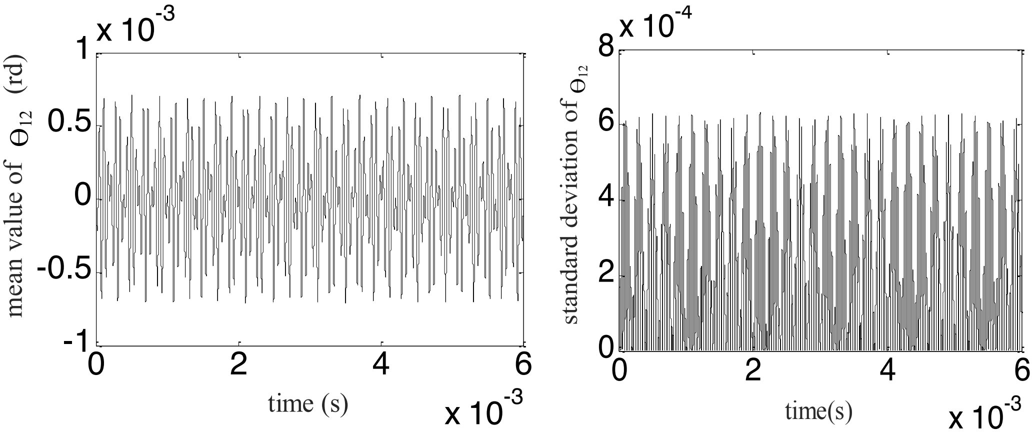


Fig.2. Mean value and standard deviation of θ12 (t)

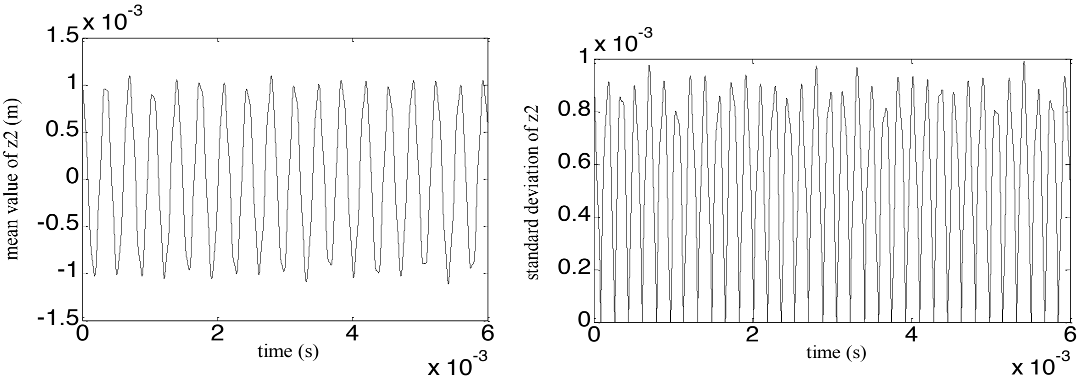


Fig. 3. Mean value and standard deviation of z2 (t)

4. Conclusions

An approach based on the polynomial chaos is proposed to study the dynamic behaviour of a bevel gear system. A complete study of the dynamic behaviour including dynamic response analyses is carried out considering 14 degrees of freedom model describing a bevel gear system with uncertainty according to the power coefficient. The main results of this study show that the polynomial chaos may be an efficient tool to take into account the dispersion of the power coefficient in the dynamic behaviour study of a bevel gear system.

5. Acknowledgements

The worked summarised here has been developed in the frame of the project CRIOS, this project has been funded by the European Regional Development Fund (ERDF) and the Normandy Region.

References

[1] Z. Hameed, Y.S. Hong, Y.M. Cho, S.H. Ahn, C.K. Song, *Condition monitoring and fault detection of wind turbines and related algorithms*, Renew. Sustain. Energy Rev. (2009) 1–39.

[2] P.Srikanth, A.S.Sekhar, 2016, *wind turbine drive train dynamic characterization using vibration and torque signals*, Mechanism and Machine Theory, 98, 2-20.

[3] Q. Guo, *Incorporating stochastic analysis in wind turbine design: data-driven random temporal-spatial parameterization and uncertainty quantification*, thesis, (2013), Digital Repository and Iowa State University

[4] Z.Y. Liu, XiaoDong Wang, Shun Kang, *Stochastic performance evaluation of horizontal axis wind turbine blades using non-deterministic CFD simulations*, Energy 73 (2014) 126-136.

[5] S. Wei, Jingshan Zhao, Qinkai Han, Fulei Chu, *Dynamic response analysis on torsional vibrations of wind turbine geared transmission system with uncertainty* .Renexable Energy 78 (2015) 60-67.

[6] Bruyère, J.Y. Dantan, R. Bigot, P. Martin, *Statistical tolerance analysis of bevel gear by tooth contact analysis and Monte Carlo simulation, Mech*. Mach. Theory 42, (2007) 1326–1351.

[7] A.S. J. Witteveen, S. Sarkar, H. Bijl, *Modeling physical uncertainties in dynamic stall induced fluid-structure interaction of turbine blades using arbitrary polynomial chaos*, computers and structures 85, (2007) 866-878.

[8] H. N. Najm, *Uncertainty quantification and polynomial chaos techniques in Computational Fluid Dynamics*, Annu.Rev. Fluid Mech. 41 (2009), 35-52.

[9] G. Kewlania, J. Crawfordb, and K. Iagnemma, *A polynomial chaos approach to the analysis of vehicle dynamics under uncertainty*, vehicle system dynamics (2012),1-26.

[10] A. El Hami, A. Guerine, T. Fakhfakh, M. Haddar, *A polynomial chaos method to the analysis of the dynamic behavior of spur gear system*, Structural Engineering and Mechanics. 53(4) (2015) 819-831.

List of Authors

APPENDIX:

Programme

56th ESReDA Seminar On
Critical Services continuity, Resilience and Security

May 23rd – 24th, 2019, Johannes Kepler University, Linz, Austria

Chairman of the Seminar

- ESReDA President Dr. Luis Andrade Ferreira,
- LCM Chief Scientific Officer Dr. Johann Hoffelner

Technical Programme Committee (TPC)

Andrews John	UK
Bukowski Lech	PL
Cepin Marko	SI
Charmpis Dimos	CY
Chateauneuf Alaa	FR
D'agostino Gregorio	IT
Demichela Micaela	IT
Efrosinin Dmitry	AT
Eid Mohamed	FR
El-Hami Abdel Khalik	FR
Ferreira Luís	PT
Kolowrocki Krzysztof	PL
Kopustinskas Vytis	IT
Kortner Henrik	NO
Lannoy André	FR
Marle Leila	FR
Merad Myriam	FR
Messias Ricardo	PT
Nowakowski Tomasz	PL
Pestana Maria	PT
Pietrucha Katarzyna	PL
Rykov Vladimir	RU
Simola Kaisa	FI
Sola Antonio	SP
Tchórzewska–Cieślak Barbara	PL
Žutautaitė Inga	LT

Local Organization Committee (LOC)

For practical local information relative to the venue, please, contact: Dmitry Efrosinin (dmitry.efrosinin@jku.at), Cornelia Brandt-Springsits (cornelia.brandt-springsits@jku.at), with Inga Žutautaitė-Šarunienė (Inga.Saruniene@lei.lt) and Mohamed Eid (mohamed.eid@cea.fr) in Cc.

Organizers

Johannes Kepler University Linz – JKU

Johannes Kepler University in Linz (JKU) is the largest research and educational institute in Upper Austria. As a young university (inaugurated in 1966) and the largest scientific institution in Upper Austria, JKU has evolved into a hub of science, industry and business in a short space of time. 60 study programmes for over 19,000 students guarantee a modern and practical education with excellent job prospects. The research activities of the faculties and institute are recognised worldwide. (www.jku.at)

Institute for Stochastics JKU

The lecture courses at the Institute for Stochastics provide an overview of relevant topics in probability theory and statistics. Further there are regularly particular courses based on the research areas of the members of the Institute for Stochastics: e.g., Time Series Analysis, Queuing Theory, Reliability Theory, Stochastic Numerics, Martingale and Brownian Motion, Markov Chains. Research areas of the members of the Institute for Stochastics comprise stochastic analysis, stochastic numerics, statistics and there applications in other disciplines. (www.jku.at/stochastik)

Linz Center of Mechatronics – LCM

Mechatronics – an intelligent fusion of informatics, mechanics and electronics. The Linz Center of Mechatronics is a reliable partner for research and development for national and international customers since more than 15 years. The LCM supports the customers from idea generation, research and development to the introduction of series production. Our infrastructure allows for the production of prototypes and small lot sizes as well as the verification of developed systems and components. The specific knowledge that the employees of LCM possess forms the basis for collaborations in research and development and the foundations to design new, intelligent, networked or autonomous systems for the manufacturing industry. The JKU belongs to the ownership list. (www.lcm.at)

European Safety, Reliability & Data Association – ESReDA

ESReDA is an international non-profit association with approximately 35 member organizations comprising companies from different industries, research organizations and universities working within the safety and reliability field.ESReDA aims to promote the development and the exchange of data, information and knowledge through the promotion of Project Groups (PG) on subjects related to Reliability, Safety and Data Analysis. In this PG's some of the best world specialists in these subjects are able to meet and, in a first time, to aggregate their knowledge and then to disseminate it for the sake of the scientific and technological communities in Europe and around the World. This dissemination can be made by organizing seminars twice per year and publishing the most important results of the Project Groups. Safety and Reliability Engineering is viewed as being an important component in the design of a system. However the discipline and its tools and methods are still evolving and expertise and knowledge dispersed throughout Europe. There is a need to pool the resources and knowledge within Europe and ESReDA provides the means to achieve this. (www.esreda.org)

Wednesday May 22nd, 2019

ESReDA Project Group Meeting (public events)

Johannes Kepler University Linz
Altenbergerstraße 69, Linz, Austria

10.00-12.00	PG on Big Data, Reliability, Risk and Safety Analysis
12.00-13.00	lunch
13.00-15.00	Joint meeting PG CI-PR / MS&A-Data and PG on Resilience Engineering and Modelling of Networked Infrastructure
15.00-18.00	BoD meeting

Participation is free and open to all experts, engineers and researchers interested in the topic. For logistic reasons, would you please send your interest expression by mail to Inga Žutautaitė-Šarūnienė (Inga.Saruniene@lei.lt), Dmitry Efrosinin (Dmitry.Efrosinin@jku.at) and
Mohamed Eid (mohamed.eid@cea.fr).

Programme

1st day, Thursday May 23rd, 2019

08.00 – 08.30	**Registration**
08.30 – 09.00	**Welcoming Session**
09.00 – 10.00	**Keynote Paper** Chair: Pr. Luís Ferreira Towards an ecosystem of models - Common visions of automated engineering and critical infrastructure modelling *Pr. Johann Hoffelner*
10.00 – 11.20	**SESSION 1: S1 - CI Interdependency & Disruption Risk Analysis** Chair: Dr. Kaisa Simola, Pr. Dimos Charmpis Challenges to protect critical energy infrastructure *Vytis Kopustinskas, Marcelo Masera , Ricardo Bolado-Lavin* Advances in vulnerability assessment of coupled gas and electricity transmission networks by using graph theory *Jose M. Yusta, Jesus Beyza, Jose A. Dominguez-Navarro, Rodolfo Dufo, Jose L. Bernal-Agustin* Recoverability analysis model for railway networks *Ratthaphong Meesit, John Andrews, Rasa Remenyte-Prescott*
11.20 – 11.40	**Coffee Break**
11.40 – 12.40	**SESSION 2: S2 - Systems & Processes Performance Modelling** Chair: Pr. Cyp F.H. van Rijn, Dr. Vytis Kopustinskas Prevention of thermal runaway risk in chemical process industries infrastructure by using model-based fault detection and diagnosis methods *Amine Dakkoune, Lamiae Vernières-Hassimi, Lionel Estel, Dimitri Lefebvre* A Polynomial Chaos method to the analysis of the dynamic behaviour of Vertical Axis Wind Turbine *Abdelkhalak El Hami, Imen Bel Mabrouk*
12.40 – 14.00	**Lunch**

14.00 – 15.20 **SESSION 3: S3 - Continuity, Disruption Modelling & Resilience**
Chair: Dr. Kate Sanderson, Pr. Abdelkhalak El Hami

Evaluation of the power system reliability considering the renewable sources
Marko Čepin

Modelling resilience of complex engineered systems using service continuity approach
Lech A. Bukowski

Models of information influence for assessing information systems security
Igor Goncharov, Nikita Goncharov, Pavel Parinov

Simulation-driven approach for measuring risk and resilience in the network of critical infrastructures
Stefan Schauer, Thomas Grafenauer, Sandra König, Stefan Rass

15.20 – 15.40 Coffee Break

15.40 – 17.00 **SESSION 4: S4 - Mathematical Modelling of System Performance**
Chair: Dr. Dmitry Efrosinin, Dr. Stefan Schauer

Markov chain model for floods and earthquakes
Mario Lefebvre

Refining stochastic models of critical infrastructures by observation
Stefan Rass, Stefan Schauer

On sensitivity of reliability and risk models to shape of their elements
N. Kuznetsov, G. Popov, V. Rykov

17.00 – 18.30 ESReDA General Assembly

19.30 Gala Dinner

2nd day, Friday May 24th, 2019

09.00 – 10.00

Invited Lecture
Chair: Pr. Marko Čepin

Risk and reliability engineering for crisis management: using experience from asset management.
Pr. Cyp F.H. van Rijn

10.00 – 11.20

SESSION 5: S5 - Monitoring, Diagnosis & Data
Chair: Dr. Vladimir Rykov, Dr. Stefan Rass

Probabilistic models and methods for processing data in “smart” monitoring system to define rational preventive measures of supporting reliability and safety
Andrey Kostogryzov, Vladimir Artemyev, Jury Rudenko, Oleg Kurpatov, Andrey Nistratov, George Nistratov

Time series segmentation of linear stochastic processes for anomaly detection problem using supervised methods
Dmitry Efrosinin, Valentin Sturm

Index for asset value measure obtained from condition monitoring digitalized data interpretation. A railway asset management application.
Pablo González, Antonio Guillén, Antonio de la Fuente, Eduardo Candón. Pablo Martínez-Galán, Adolfo Crespo.

Using advanced data analysis to learn from infrastructure databases: The case of the US National Bridge Inventory
Filippos Alogdianakis, Dimos C. Charmpis and Ioannis Balafas

11.20 – 11.40 Coffee Break

11.40 – 12.40

SESSION 6: S6 - Surveillance, Maintenance and Services Continuity
Chair: Dr. Stefan Schauer, Dr. Stefan Rass,

Analysis of the impact of the asset health index in a maintenance strategy
Javier Serra, Adolfo Crespo, Juan Gómez, Antonio Sola

Degradation analysis and preventive maintenance modelling and assessment for improved resilience of critical infrastructures – Application to Torrent Checkdams
Chahrour Nour, Hariri Sleiman, Tacnet Jean-Marc, Bérenguer Christophe

12.40 – 14.00 Lunch

14.00 – 15.20 **INTERACTIVE SESSION: S7-Climate & CI Protection**
Moderator: Mr. Antonio Sola
Speaker: Dr. Jed Cohen

Effect of global warming on willingness to pay for uninterrupted electricity supply in European nations
Jed Cohen, Klaus Moeltner, Johannes Reichl and Michael Schmidthaler

15.20 – 15.40 **Closure Session & Next Event**
ESReDA General Secretary

KJ-NA-29989-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

Publications Office
of the European Union

doi:10.2760/23760

ISBN 978-92-76-13359-9