Maintaining confidence Dynamic Risk Management for enhanced safety

Bruno Declerck, Anje Deschoolmeester, Zina Brik

Maintenir la confiance
Gestion dynamique des risques pour améliorer la sécurité

Maintaining confidence
Dynamic Risk Management for enhanced safety

Bruno Declerck, Anje Deschoolmeester, Zina Brik
DNVGL France
69 rue du Chevaleret
75013 Paris
+33 (0)1 44 24 40 13
+33 (0)6 86 75 99 29
bruno.declerck@dnvgl.com

Résumé

Le but de cet article est de présenter les concepts et des outils développés par DNV GL pour des méthodes d'évaluation des risques dynamiques et en temps réel. Les conditions changent au fil du temps, de nouvelles connaissances deviennent disponibles et les changements de contexte peuvent affecter notre tolérance au risque. Les modèles de risque ne sont que des approximations de la vie réelle. Pour fournir une aide à la décision pertinente et au bon moment, les modèles doivent prendre en compte les conditions et le contexte d'exploitation actuels. La gestion de la sécurité de systèmes complexes dynamiques nécessite donc une évaluation dynamique des risques. Le défi consiste à donner un sens aux données collectées pour améliorer la gestion des risques. Cette dernière nécessite que les données de surveillance soient replacées dans leur contexte via un modèle de risque, afin d'évaluer la manière dont les changements affectent le risque. Le modèle mathématique s'appuie sur une approche "nœud papillon" utilisant les arbres d'événements. Le model de calcul de risque initial suppose une disponibilité des barrières de 100%, le risque effectif est mis à jour en fonction du statut réel de la barrière.

Summary

The aim of this paper is to demonstrates concepts and tools developed by DNV GL for dynamic and real-time risk assessment methods.
Conditions change over time, new knowledge becomes available, and changes in context may affect our risk tolerability. Risk models are just approximations of real life. To provide relevant and timely decision support, models need to keep track with current conditions and context. Managing the safety of complex dynamic systems requires dynamic risk assessment. The challenge is to make sense of the data to improve risk management. The latter requires that condition monitoring data is put into context with a risk model, to provide insights on how changes impact the risk. Mathematical model is based on Bow-Tie approach using event tree. Initial model Risk calculation assumes 100% effective barriers, the actual Risk is updated with barriers status considering field data.

1. Introduction

The ISO/IEC Guide 51/2014 defines safety as "freedom from risk which is not tolerable"[1]. Per this definition, to determine if an activity is safe, one requires a description and an evaluation of risk. The Society for Risk Analysis provides several conceptual definitions of risk, including: "risk is the consequences of activities and associated uncertainty", and "risk is the potential for realization of unwanted, negative consequences of an event".[2] ISO defines risk as "the effect of uncertainty on objectives".[3] While emphasizing different aspects, the essence of all these definitions is that risk is a combination of consequences and associated uncertainty. Often, the consequences considered are restricted to negative consequences, where 'negative' is defined relative to some objectives. By defining safety in terms of tolerable risk, safety is framed as a cost-benefit problem, where the negative effects of an activity are weighted against the perceived benefits. This view on safety is articulated by the principle of ALARP: that risk should be maintained 'as low as reasonably practicable', i.e. that risk should be reduced until the sacrifices necessary to reduce it further become disproportionate to the risk to be avoided.[4]

A Quantitative Risk Analysis (QRA) is commonly used for assessing risk related to concept selections and design decisions[5]. It should (in principle) cover all possible future scenarios for the asset during its entire lifetime. In practice, a QRA relies on a series of simplifying assumptions, when selecting the scope and models and risk measures to use. QRAs typically report risk in terms of time- and uncertainty-weighted averages, representing a static 'baseline risk'.

Going into operation, the baseline risk level associated with the activity is presumably judged tolerable and compliant with safety requirements and regulations. However, while a QRA presents risk in terms of static risk measures, operational conditions will, of course, vary over the asset's lifetime, and, be adapted to the type of decision and the time-horizon of the decision faced during operation.

During operation, the concerns of the operator can broadly be grouped into two categories:

1. Is the asset (still) safe?
2. How should the asset be operated (i.e., how should processes be controlled and activities scheduled and coordinated) to ensure that it remains safe while production is optimized?

The former relies on diagnosis of the current condition of the asset, while the latter relies on forecasts of the consequences of various decision options.

Historically, diagnosis of the asset condition was primarily based on inspections of the asset and testing of safety equipment, and the challenge has been that important changes, such as degradation or weakening of safety barriers, remained largely undetected – at least outside inspection intervals. In addition, the failure frequencies used in risk assessments and as input for planning inspections, tests and maintenance, are typically based on generic failure databases, which do not account for the actual operating conditions of a particular asset. However, although QRAs are usually updated at 1-5 year intervals, a QRA does not provide the level of detail or account for the actual current

conditions and temporal variations that are important for decisions during operation.

Today, with the increasing presence of sensors and abundance of data about production systems, safety barriers and various operational parameters, risk management is entering a new paradigm. Uncertainties that were previously difficult to resolve therefore, the potential for adverse consequences (i.e., the risk level) is not constant over time. For example, safety-critical barriers may degrade over time, production conditions and the production will change, and the asset itself may undergo modifications. Activity levels, hot work, environmental conditions etc. can vary on monthly, daily and hourly basis – or even from second to second. In addition, new knowledge may become available, which may reduce uncertainty or change how risk is understood. Furthermore, changes in the organizational, social or regulatory context, as well as changes to business objectives, may affect how the tolerability of risk (i.e., safety) is judged by various stakeholders.

A specific risk measure only highlights particular aspects of risk, which may be important for certain types of decisions. Meanwhile, additional aspects of risk may be 'hiding' behind assumptions made in the risk assessment. While ranking of risk according to risk measures can support decision-makers in differentiating between decision options, the ranking of risk may be sensitive to the choice of risk measures and other choices and assumptions made in the risk assessment. This affects how confident a decision-maker can be about decisions – and confidence in results can be equally important as the results themselves.

When bringing the risk assessment into operation, a key question is therefore: How do we maintain confidence that the asset is safe? One part of the answer is a good quality risk assessment during the design phase, to establish the baseline risk, and to keep that assessment updated during operation. However, it is also paramount to include the dynamics of the assumptions themselves, as the hidden risks may become important risk contributors as conditions evolve over time. In addition, the time resolution of the risk measures and information going in to a risk assessment must may now be pinned down, allowing better understanding of the current situation – throughout the value chain. New data streams, together with advanced analytics, may increase our phenomenological understanding and improve our ability to predict the evolution of processes, such as equipment degradation and failure. With regards to communication of risk results, new digital platforms allow more interactive presentations of results, and increased computing power will allow simulations of scenarios to be performed on demand during operation to evaluate the consequences of various decision alternatives.

DNV GL is working to make risk assessment more dynamic and suitable for informing decisions in operation. By this, we mean risk assessments that are updated based on the latest knowledge, able to capture important time-dynamics of risks, and flexible with regards to answering new questions that may arise during operation. Part of the solution is to take advantage of new technologies, to update existing risk models in real time, and to make results available to customers on digital platforms. However, advances must be rooted in a fundamental understanding of what risk is, the dynamics of risk and the specific needs of decision-makers during operation. This becomes particularly important with the development of more remotely operated and autonomous systems, where a key question will be: which decisions can and should be automated?

This paper describes some of the novel methods and tools from DNV GL on dynamic risk management.

2. Dynamic Barrier Management (DBM)

The barrier risk management approach has been in use in aviation, rail, and oil & gas industries for more than 15 years, and for even longer in the nuclear industry where it is termed Defence in Depth [6]. The underlying theoretical basis links well to the swiss cheese analogy (Reason, 1997) where threats (or hazards) continuously challenge a system, with safety barriers being slices of cheese and their reliability or effectiveness indicated by the number and size of holes. An incident occurs when all the holes line up and the threat can directly reach the consequence. Intuitively, a system is safer with more barriers and smaller holes.

Barrier management has been a key concept in the management of major accident hazards (MAH) in the operational phase across the process industries since the early 1990s. Incidents such as Piper Alpha (1988), Texas City (2005), and Deep Water Horizon (2010) all contributed to step changes in adoption of barrier management thinking and methodologies. This barrier management approach takes barriers identified and assessed in the design stage and implements a management strategy throughout the facility lifetime.
With the shift from prescriptive to goal-setting safety legislation, regulators increasingly considered barrier management as a tool to ensure companies managing major hazards could demonstrate control of their associated risks. Similarly, the industry saw barrier management as the mechanism to actively measure risk management performance and reduce the likelihood of loss and litigation.

Barrier programs when originally developed assume all barriers are functioning well – at their performance standard (which allows for some probability of failure of demand – PFD; these are the holes in the swiss cheese). But in reality, barriers degrade with time. They can perform below their assumed PFD and the overall system's safety will thus be less than predicted by the initial risk analysis. If not actively managed, and unless suitable remediable actions are taken the risk levels will be higher, perhaps much higher, then assumed.

Different barriers also provide different risk reduction and degrade at different rates.

A common approach to safety barrier management is risk-based inspection (RBI), whereby barrier status is monitored by audits and inspections whose frequency is determined by the additional risk that would be created if a particular barrier failed. Traditional barrier management techniques do not adequately capture the dynamic nature of this degradation, and it does not link barrier status to a risk impact. As such, barrier management is constrained by the fixed frequency of maintenance, testing, inspection, audit and other intervention activities.

The concept of dynamic barriers and their impact on risk is shown in Figure . The lower left side of this figure shows barrier status – initially at full level, but dropping in steps as various barriers degrade, upticks show barrier maintenance repairing barriers, but overall during operations the holistic barrier status has fallen below the initial commissioning level. The dotted green line shows knowledge of barrier status only slowly being updated as preplanned cycles (eg. planned inspection programs ,..) address degraded barriers. The impact is shown on the upper left – as barriers degrade the risk level increases. Risk levels go up and down as barriers degrade and later get repaired. The average risk level is well above the target, and for short intervals can be very high until relevant barriers are repaired. The figure is conceptual as some barriers have greater importance than others and so the risk and barrier status are not simply inverse views of the same thing, although in general they follow this trend.

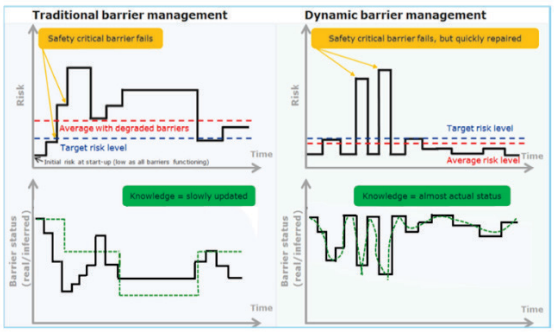

Figure 1. Relationship between barrier status and overall risk level

The right side of Figure shows the effect of dynamic barrier management. The barriers here also degrade, but management is aware of the degradation much sooner and can initiate repairs, avoid activities or implement equivalent measures much more quickly. The impact on risk is much better – spikes still occur as safety critical elements degrade, but since these are fixed quickly, risk levels revert to desired levels also quickly and the average risk meets the target risk level.

Dynamic barrier management (DBM) is a new paradigm, where information from a multitude of sources is collected, analysed and visualized in real time, or near-real time, to provide better understanding of barrier status and to enable decision-makers to manage barriers and risk more effectively. Both aspects, barrier performance management and cumulative risk management, offer benefits in their own right, but they become much more powerful when they are linked together into a DBM process.

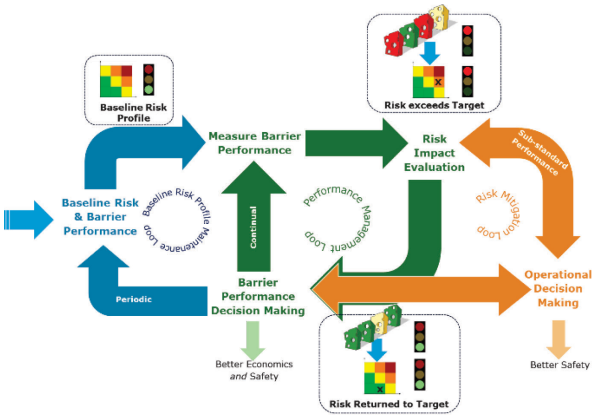

Figure 2. High level DBM process

A high level DBM process is made up of 3 interacting cycles operating at different frequencies:

1. Performance Management Loop
2. Risk Mitigation Loop
3. Baseline Risk Profile Maintenance Loop

It should be noted that cumulative risk management requires adequate barrier performance management to be in place to work effectively. As such, when very limited systems are in place, barrier performance management would be a good place to start with DBM. After building confidence in the barrier performance management system one could then be encouraged to develop a cumulative risk management process on top. However, if the existing barrier performance management processes are suitable, then a cumulative risk management process may be built on top of that foundation.

The different practical building blocks of a DBM approach are represented in below figure.

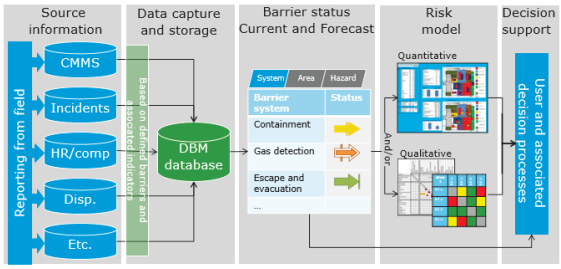

Figure 3. DBM approach

Following sub-processes are needed:

- Barrier Identification, Importance Ranking and Dependencies.

The foundation of any barrier management system requires the identification and documentation of all relevant barriers and their performance requirements. There is much work that has been done in this area in the process industries over recent years and so it is expected that most clients will have some understanding of their available barriers. Many will also have implemented some form of measurement process to monitor barrier performance.

In addition, it is necessary to have knowledge about the barriers importance, i.e. the effect of degraded barrier performance on the risk profile.

In mathematical terms, barrier importance can be expressed as

$$barrier\ importance = \frac{Risk\ when\ barrier\ is\ failed}{Risk\ when\ barrier\ is\ at\ its\ PS} \quad \{1\}$$

With P.S meaning Performance Standard

for which the computed risk is in the form of some risk measure. These importance weights should be a number higher than 1, reflecting the increase factor on the risk level when the barrier is not functioning.
There will also be different kinds of dependencies between barriers which is also relevant to have knowledge about when evaluating different barrier status contribution to the risk level.

- Measuring and Evaluating Barrier Status

Barrier status refers to the degree of compliance with the performance expectations associated with a particular barrier. This is important to understand because degraded barriers offer a reduced risk reduction benefit and hence risk levels are no longer at expected baseline levels. Measuring the status of barriers is challenging and within industry is generally achieved through the use of performance indicators. The development of process safety performance indicators is thoroughly addressed in the literature and several guidelines have been issued over the last decade. In particular, the guideline "Development of process safety indicators - A step-by-step guide for chemical and major hazard industries"[7] is commonly used and referred to.

Finally, predicting barrier status is a necessary capability for unlocking the potential of DBM. The purpose for prediction analysis, or prognostics, is to make qualified predictions of future behaviour and statuses from the current and historical barrier status data that could help in avoiding barrier degradation or/and potentially accidents. It is important for two reasons:

1. It allows a more representative picture of overall status of barriers today given that status data may be arriving at different frequencies and that data is only accurate at the time it is measured. This supports tactical, operational decision making.
2. It allows forward prediction of barrier status to some point in the future which supports more effective planning and strategic decision making.

- Cumulative risk

Over time the performance of the barriers degrades at different rates and in different ways. The net effect of this is to increase the baseline risk level to a residual risk level. It is this residual risk level that the Cumulative Risk Management approach estimates. In most cases, semi-quantitative methods give already a good picture of the relative risk measures. At the highest level of sophistication, the changes in barrier status can be plugged into a (detailed) quantitative risk model that automatically calculates the corresponding change in absolute risk measures.

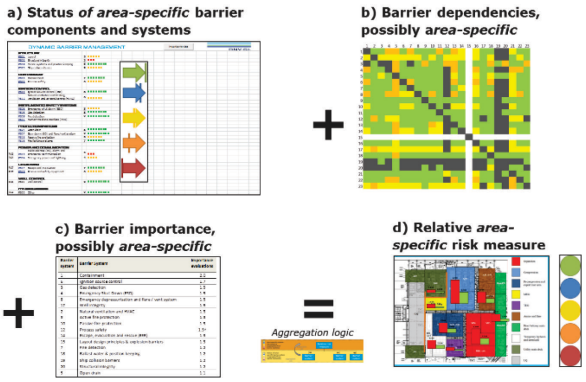

Figure 4. Cumulative risk

DBM can contribute to increased safety performance with same or lower cost.[8] It improves decision support for prioritizing critical maintenance, implementing compensating measures, and for day-to-day risk analysis. By ensuring more regularity during operation, DBM supports both asset safety and operational efficiency, by avoiding process upsets. Early indications of barrier degradation provide flexibility for the scheduling of small, multiple corrective actions rather than intrusive and large ones.

The limit of this model is related to uncertainties of the evaluation of the status of each barrier and the impact on the Probability of Failure on Demand of the barrier.

2.1 Example of impact of degraded safety barrier on scenario risk

To illustrate the approach a generic example is used. The hazard might be assumed to be hydrocarbon gas under pressure, and the top event is then loss of containment, but this is not critical for the example.

The bowtie has two initiating events, a and b, and two outcomes, A and B.

On the left-hand side are two preventive barriers, P1 and P2, and on the right, are two reactive barriers, R1 and R2.

Not all barriers are effective against all threats, nor against all consequences. For the purposes of this example the bowtie is built as follows to represent how a typical case might look.

From the example bowtie, there are two threats and two consequences, so four lines. These lines are represented as follows:

aA	fa.P1.P2.R1.CA	0.005
aB	fa.P1.P2.R1.R2.CB	0.0001
bA	fb.P1.R1.CA	0.25
bB	fb.P1.R1.R2.CB	0.005

The total risk represented in this bowtie is therefore: 0.2601 units of harm per year.

Note the use of the term “units of harm” to avoid confusion with absolute risk measures.

As a diagram, the bowtie is populated as follows:

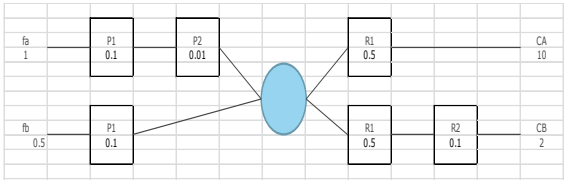

Figure 5. Example 1

Barrier P1 is degraded, such that it now has probability of failure of 50%

The modified bowtie diagram is as follows (grey values represent the base case)

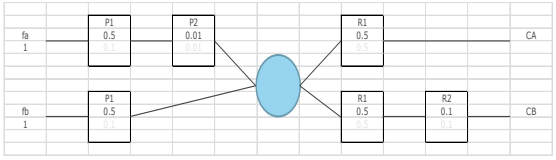

Figure 6. Example 2

The modified expectation values are as follows:

	Initial	Current	Delta
aA	0.005	0.025	400%
aB	0.0001	0.0005	400%
bA	0.25	1.25	400%
bB	0.005	0.025	400%
	0.2601	**1.3005**	**400%**

The expectation value from this bowtie has increased from 0.2601 to 1.3005, an increase of 400%.

3. MyQRA

A Quantitative Risk Assessment (QRA) is a formal and systematic approach to estimating the likelihood and consequences of hazardous events, and expressing the results quantitatively as risk to people, the asset, the environment or business. It also assesses the robustness and validity of quantitative results, by identifying critical assumptions and risk driving elements. A QRA is a central input for determining design requirements, operational restrictions and the need for preventive or mitigative safety barriers.
While QRA reports are comprehensive and static, offering certain information at a fixed point in time, QRA’s generate additional information that can be of significant additional value and a lot of times hidden for the end users in many comprehensive tables and numbers. In both capex and opex phases of an asset’s life cycle, safety-critical choices are sometimes made based on an outdated risk-picture, without sufficient comparisons of design and operational options.
MyQRA harnesses this, unlocking the detailed information from QRA studies in ways not possible in a typical static report. It allows users to view and interact with information more

tangibly, using filtering, drill-down functionalities and 3D visualizations.

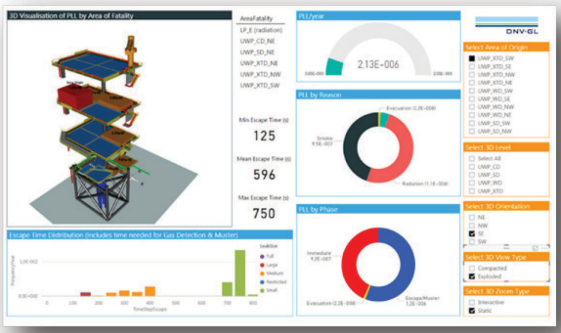

Figure 7. Interactive QRA results

All latest QRA's (reports, interactive results, and other related) deliverables are securely stored in one easy to access location on a secure database in accordance with industry best practice and to ISO 27001 standards.

Through MyQRA, safety critical decisions during design and operations can be made easier with side by side comparisons of different design and modification options based on current risk picture. Cloud QRA enables online sensitivities on all input data and fast access risk results from QRA studies. It will allow different stakeholders in design or operational phase to perform 'what if' scenarios for better-informed, risk-based decisions. MyQRA could therefore by used as part of ALARP demonstrations, to easy test out certain alternative options or perform a cost-benefit analysis. Users can determine risk drivers, isolate single events and perform filters to understand risks far better than a static report could describe.

MyQRA can be used to support decisions and communicate risk across the lifecycle of a project. It can also be accessed by all project stakeholders, helping to avoid disconnect between the parties involved. MyQRA enables both technical and non-technical oil and gas professionals to better understand hazards, particularly in the handover from capex to opex phase, to enhance risk communication and thus to make day-to-day decisions more effectively.

4. Conclusion

This paper has discussed the dynamics of risk and the need for more interactive and dynamic risk assessments. Specifically, DNV GL believes that:

- Managing the safety of complex dynamic systems requires dynamic risk assessment, the ability to learn from experience and adapt to new conditions. There is a need to take a top-down systems perspective when assessing risk, acknowledging the complex interaction between human, technology and organization.
- Aspects that are uncertain in design risk assessments may become known during operation. Decisions made during operation must reflect actual conditions of production, the status of safety barriers, environmental conditions, etc.
- Making risk assessments dynamic involves more than updating risk measures based on current conditions – it includes continuous monitoring and evaluation of the validity of all underlying assumptions, which may hide aspects of risk.
- The increasing presence of sensors, the abundance of data and rapid development of machine learning today is only beginning to transform how safety is managed. Going forward, our ability to enhance safety depends on our ability to extract relevant knowledge from data, which in turn depends on our models and domain knowledge.

Combining the power of past knowledge with new dynamic risk models, data analytics and new ways of controlling risks, we may see a paradigm shift in accident statistics: Expanding from merely assessing risk to controlling and managing risk shifts the focus from accident statistics to dynamics leading to accidents. From this, more accidents can be avoided. Ultimately, we may even have a vision of avoiding accidents altogether.

Some examples of new methods and tools developed by DNV GL to address these challenges have been presented here:

- Dynamic barrier management – a new barrier management strategy making use of real-time data to monitor and maintain the integrity of safety barriers.
- MyQRA – DNV GL's new online service which unlocks the detailed information from QRA studies in ways not possible in a typical, fixed report.

In addition to the above, more projects on dynamic risk management are underway within DNV GL and with our customers and partners in various industries to develop better tools to support decisions in operation and to enhance safety in the industries we serve.

5. References

[i] International Organization for Standardisation and International Electrotechnical Commission, "ISO/IEC Guide 51:2014: Safety Aspects – Guidelines for their inclusion in standards", 2014
[ii] Society for Risk Analysis, "SRA Glossary", 2015.
[iii] International Organisation for Standardization, "ISO31000-Risk Management", 2018.
[iv] Health and Safety Executive UK, "ALARP at a glance",
[v] DNV GL, "Maintaining Confidence: Dynamic risk management for enhanced safety." Available : https://www.dnvgl.com/oilgas/download/position-paper-maintaining-confidence-dynamic-risk-management-for-enhanced-safety.html
[vi] DNV GL, "Enhancing offshore safety and environmental performance." available: www.dnvgl.com/oilgas/offshore-safety.html
[vii] Health and Safety Executive UK, "Development of process safety indicators - A step-by-step guide for chemical and major hazard industries", 2006
[viii] DNV GL, "A smarter way to avoid incidents and save costs." Available https://www.dnvgl.com/oilgas/perspectives/a-smarter-way-to-avoid-incidents-and-save-costs.html