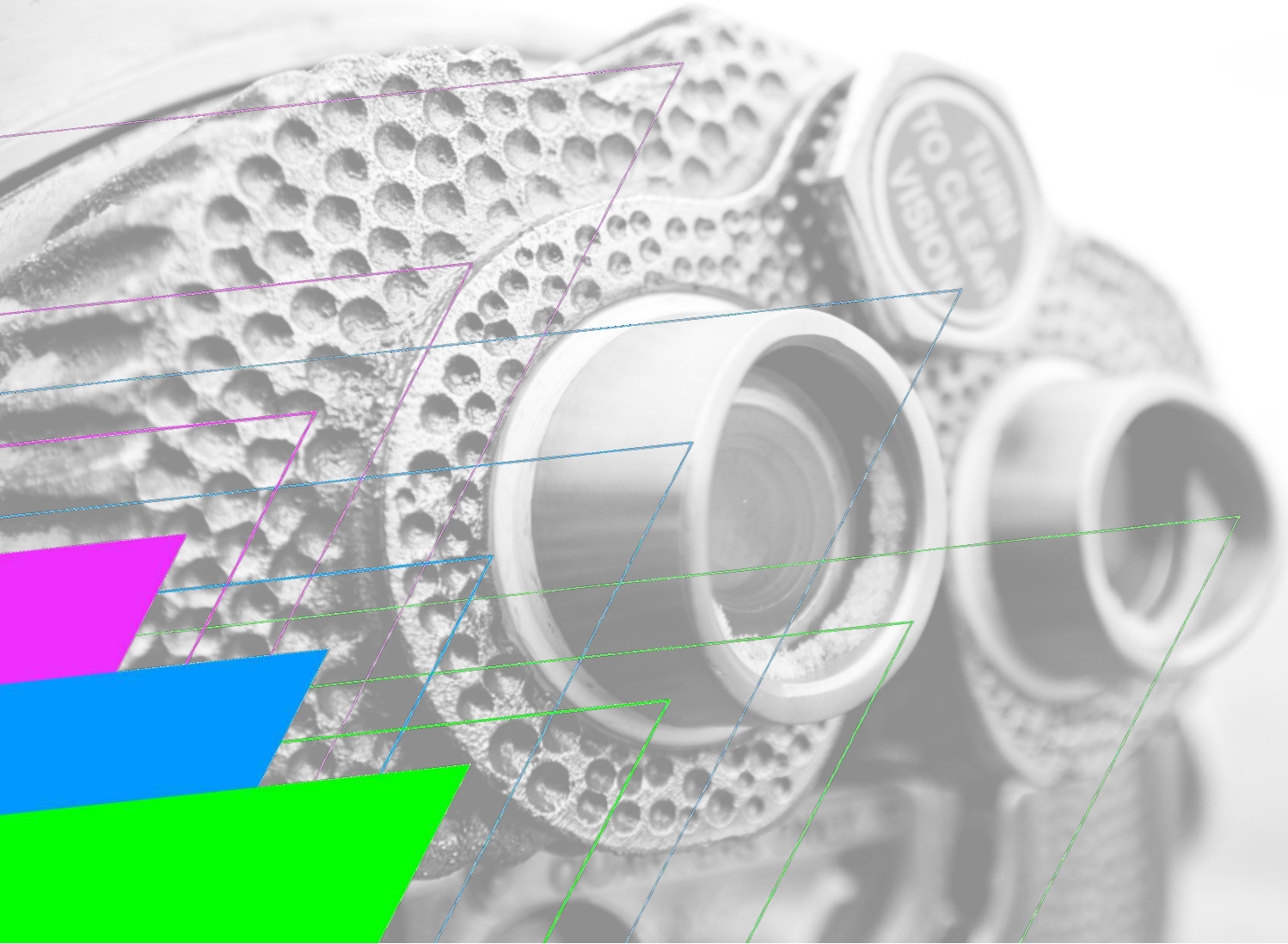
Enhancing Safety: The Challenge of Foresight

ESReDA Project Group *Foresight in Safety*



Chapter 9

Safety foresight in asset management

Paulo Maia
John Kingston

ESReDA
European Safety, Reliability & Data Association

Table of contents

9 Safety foresight in asset management

Paulo Maia, Energias de Portugal (EDP) – Gestão da Produção de Energia, S.A., Portugal,
John Kingston, Nordwijk Risk Initiative Foundation (NRI Foundation), The Netherlands.

Executive summary

In recent years, *asset management* has been applied consistently as a structured discipline to several areas of economic activity, including infrastructure, industry, banking and insurance. Banking and insurance are mainly related to the financial sector. Infrastructure refers to energy networks (electricity, gas, district heating), water and sewage, roads, rail network and telecommunications, and the relevant industrial sectors include, amongst others, power generation (renewables, fossil and nuclear), chemical and petrochemical, and pulp and paper. However, to present this subject in a reasonable level of detail, only industrial assets will be considered here, with a special attention to the power generation industry.

There are many reasons why asset management has recently become an essential part of management activities and management science. Several examples can be cited, such as the ageing of industrial asset systems and its increasing integration; more stringent quality, safety and environmental requirements for the industry, imposed by regulators; greater awareness of risks among workers, managers and stakeholders; globalisation and fierce market competition; and pressure on asset managers for higher profitability and return on assets. Frequently, several of these features generate a combined effect, making it difficult to identify the specific contribution of each one to asset management.

In the literature, several definitions of asset management can be found. However, the definition included in the ISO standard for asset management released a few years ago (ISO 55001:2014), will be used here as a reference, although its meaning is quite broad. The standard defines asset management as a coordinated activity of an organisation to realise value from assets. In turn, 'asset' is defined as an item, thing or entity that has potential or actual value to an organisation. However, in the specific context of this paper, the term *asset management* has its main application to the industry, that is, asset management focussed on physical assets.

The main objective of this paper is to identify areas of asset management that can be used in safety foresight, to enable the detection process for systems/equipment deterioration signals or anomalies before a serious accident can occur. To accomplish this objective, it is necessary to limit the period of the lifecycle of an industrial asset to its intended use, that is, to the operational/production stage. However, this does not preclude taking necessary safety measures during design, or later in the construction, commissioning or even in the decommissioning stages.

The relevant activity during the operational/production stage is Operation and Maintenance (O&M), which is accomplished both by personnel and systems/equipment through a set of processes following established operating procedures. This is the reference period that will be considered in detail in this chapter, it being simultaneously the longest and the most relevant in the life cycle of an industrial asset.

In industry, although *internal agents*, including managers and technical staff, put asset management into practice every day, the role of *external agents* cannot be neglected. They influence the way industrial assets are managed, too. External agents include: regulators, certification bodies, insurance companies, technologists (high-tech manufacturers), O&M specialist companies or industry institutes, users' groups and sector associations. They help companies by identifying non-conformities, weaknesses, gaps and process deviations in the way asset systems are being managed. When agents find these indications, they act: issuing instructions and alerts, or making recommendations aimed at correction. And occasionally, recommendations issued by one external agent can even induce a synergistic effect on related issues in the domain of other agents. As the contribution of these external agents to foresight in safety is not usually mentioned in the literature, it will be the main topic addressed in this chapter. To better illustrate the subject, practical examples taking from the conventional power generation industry are given. In this context, nuclear power generation is ruled out of this analysis, as oversight of regulators is quite intense, even dominant in respect to other external agents, and major accidents occur very infrequently. As a result, it is quite difficult to find areas for improvement in nuclear power generation that would have broad application to other industry sectors.

9.1 Introduction

"I am prepared for the worst, but hope for the best."
Benjamin Disraeli (1804-1881)

The term 'asset management' has become quite popular in recent years and is currently used to address management issues in several areas of economic activity, including infrastructure, industry, banking and insurance. Although asset management activities have been performed since society started to use capital assets, recent changes in our way of living and business environment have required the adoption of a more structured management approach. The efforts made to obtain this more structured approach culminated with the publication in 2014 of the first edition of the ISO standard on asset management Standard 55001. The standard defines a set of requirements that once established, implemented and maintained, will ensure the fair asset management performance of an organisation, responding to the requirements and expectations of interested parties and ensuring value creation and maintenance.

Assets can be physical, financial, human or 'intangible'. However, to reduce the broad spectrum of assets to be addressed in this chapter, only physical and human assets from the industry sector will be considered. Physical assets include systems and equipment, the environment and the associated production processes. Special attention will be devoted to the conventional power generation industry, from which examples will be provided to further illustrate the statements and, hopefully, enabling replication to other industries, whenever applicable. Nuclear power generation is ruled out of this analysis, for several reasons, including the specificity of this industry and the intense oversight of regulators, mainly concerned with nuclear safety. As a result, it is quite difficult to find areas for improvement in nuclear power generation that would have broad application to other industry sectors.

The main objectives of this chapter are to (i) identify tools, practices and agents (internal and external) that can contribute to safety foresight in asset management within the power generation sector, and (ii) to describe how this can be achieved.

9.2 Systems and Equipment

In the power generation industry, as in other industries, physical assets can be divided into several categories and levels. Complementary to this, a coding system is usually adopted for asset management purposes, including operation and maintenance. At the top level, power plants are divided into units, of similar or different design, technology, installed capacity, etc. When a power plant is to be constructed within a specific investment project, typically between two and four units, similar units are considered. The division into units provides adequate operational flexibility to satisfy power grid needs and minimise the risk that all units might fail simultaneously. However, in recent years, as an effect of the European liberalised electricity market and the opportunity to use extra installed capacity, some reservoir hydro power plants have been subject to repowering projects. In these cases, the tendency is to construct units with a higher installed capacity, thereby taking advantage of the benefits of a higher electricity price in peak hours and, simultaneously, of the technological advances made in relation to the original units, which sometimes were built decades before.

The second level of physical assets are the systems and equipment; the third, the components; and fourth, the parts.

Having in place an efficient coding system is a key-element for operation and maintenance activities. It enables the asset owner to better manage systems and equipment failures, stocks of critical spare parts, and communication with manufacturers.

Reference to all these asset levels will be made, where appropriate.

9.2.1 Operation

9.2.1.1 Performance Requirements

Systems and equipment performance requirements are established through a set of standards, manufacturer operational instructions and emergency procedures that should be followed by the industrial asset personnel, including managers, supervisors and operators.

Any advanced industrial process is managed by a command and control system, usually known by the acronym SCADA (Supervisory Control and Data Acquisition). This system includes safety instrumentation and process control systems that are

run automatically, under operator supervision. In recent years, major advances have been made in those systems. Due to this, command and control system obsolescence cannot be ignored, as this system is the 'heart' of the plant. Based on experience, a command and control system becomes obsolete approximately in 20 years. This is critical, especially for hydro power plants, as these power plants may reach 100 years, without major improvements in the remaining systems, besides regular maintenance overhauls.

Operators should be submitted to a specific training programme in accordance with their own functional requirements, comprising theoretical courses and on-the-job training. A simulator aided operator training through a dynamic operator training system can improve and speed up this process significantly, enabling the trainee to repeat actions that were not performed correctly until an acceptable performance level is reached. Depending on the functions allocated to each operator, in some cases, training can last one year, before being able to run a unit autonomously. Refresher training sessions should also be delivery periodically, to check if appropriate actions are taken, when an immediate response is required. Although human error cannot be eliminated, training is one key aspect to lower the operational risk, especially during emergency situations, when human factors are at stake and a swift and appropriate response from plant operators is intended and expected.

9.2.1.2 Safety Requirements

9.2.1.2.1 Procedures

Safety alerts are included in the operating instructions set out by systems and equipment manufacturers (technologists). The Emergency Safety Plan (ESP) should also be readily available to all personnel, preferably both on paper and electronically, in the internal information technology network.

The ESP provides details about the actions required in the event of emergency situations. Usually, foreseeable loss scenarios are included and selected as the basis for periodic safety drills. The main purpose of drills is to test the preparedness of the industrial asset personnel to react to a specific emergency and limit the damage. Drill results highlight areas for improvement and allow corrective actions to be scheduled and included in the safety drill report [see also chapter 5].

Other relevant safety procedures that might be available are referred in 9.3.2.3.2.

9.2.1.2.2 Proactive Controls

Proactive controls include alarms, emergency or unplanned shutdowns (trips), proactive safety performance indicators, and event analysis. Under certain circumstances, they can be interpreted as early warning signs (EWS) of system malfunction (instantaneous) or as system safety deterioration (over time), when a benchmark or reference parameter indicating a normal operation situation can be established [see also chapters 6, 7 and 10].

In operational safety, an alarm activation means that an anomaly has been detected in the system or equipment and an urgent action is required to eliminate the cause. Alarms are installed in systems and equipment to allow actions to be taken well in advance of a more serious event. These include actions on a process variable, machinery malfunction, fire outbreak, etc.

In terms of process control, an alarm is an indication to the operator that is initiated by a process variable or measurement that has passed a predefined limit considered to be an undesirable or an unsafe value. Poorly functioning alarm systems, or lack of training operating a system or equipment under emergency situations, worsen the seriousness of upsets, incidents and major industrial accidents.

Alarm activation can be attributed to two main sources: operator error or equipment malfunction. False alarms may also occur, either due to a non-calibrated or faulty sensors. To overcome this situation, where critical parameters on critical systems and equipment are concerned, the '2oo3' (2 out of 3) voting system principle should be applied. Under these circumstances, this principle will issue a shutdown command if at least two modules (that is, modules of critical parameter sensors) issue a shutdown command. This voting system will fail to perform its intended function on demand if two failures occur together. In addition, both failures will have had to be undetected by the system's internal diagnosis; or one failure must be 'dangerous undetected' and the other failure has to be 'dangerous detected'. When two dangerous and detected failures occur, it is assumed that the system responds in a safe way, and a system trip will occur. This can be considered the means of last resort for the system to prevent a potential serious failure.

In fact, trips are the last resort available to halt the system operation, to avoid further deterioration and potential widespread damage to equipment or harm to personnel and the environment. This action can be triggered by human

intervention (the operator) or automatically by the system, when predefined operational parameter values are reached. The costs of trips, which happen more frequently than accidents, can be quite significant. Besides process interruption, that can only be resumed after the possible cause of the unplanned shutdown is well identified and corrected. Also, although a more serious failure has been prevented, an unplanned shutdown reduces slightly the useful life of equipment. When an abnormal event is stopped before causing any damage and the operational parameter returns to its normal zone, this is considered as a process near-miss.

To take full advantage of the information provided by such indications of system disturbances or malfunctioning, alarm and trip analyses (also called event analysis) are highly recommended.

Many industrial companies record these alarm occurrences in distributed control systems (DCS) and emergency shutdown (ESD) databases. Operators, supervisors and managers seek guidance from these databases, by recording key indicators and paying special attention when alarm flooding occurs (Oktem, *et al.,* 2013).

Asset managers are becoming increasingly aware that these databases are rich in information related to near-misses. In recent years, researchers have been developing key performance indicators or metrics, associated with potential trips and accidents, leading indicators and failure probabilities of each of the safety systems. When conducted at frequent and regular intervals, analyses that are associated with these performance indicators are usually referred to as dynamic risk analyses or simply near-miss analyses.

9.2.1.2.3 Reactive Controls

Reactive controls are actuated when an unwanted event materialised and an immediate response is needed to limit the damage to a system, equipment, property or even harm to people and environment. Contrary to the proactive controls, where no or limited damage is expected, reactive controls are the last resort. An asset manager implements reactive controls to prevent an incident escalating to the degree where widespread damage and great financial loss would result. Typical examples on the conventional power generation industry are automatic or manual fire protection systems, dam spillways, fire brigade action, and also drills (derived from accident scenarios) conducted to assess the emergency preparedness of power plant personnel and reactive safety performance indicators. The main objective here is to react, in the shortest time possible, to suppress the source of danger with maximum effect. Even if limited damage has occurred due to the swift action of first responders, the objective is to learn lessons and so prevent similar accidents. Although safety foresight was not effective to prevent this specific accident, as it was not able to assess the risk and treat it adequately, if appropriate corrective measures will be adopted, similar accidents will be prevented. However, if corrective actions were to be implemented in the system, the conditions heralding its occurrence will be detected in an earlier stage, enabling precautionary actions to be taken.

9.2.1.2.4 Safety Performance Indicators

In the literature, there is no unified approach concerning terminology and definition of Safety Performance Indicators (SPI).

An SPI can be defined as a basic parameter, described qualitatively or quantitatively, that is perceived as having potential meaning or a relationship to plant safety (Davies, *et al.,* 2006), (Hale, 2009), (Van Binnebeck, 2002).

A robust performance indicator should comprise the following features:

- Relevant: to provide useful information in due time for decision taking;
- Reliable: it provides the same value when used by different people;
- Measurable: able to be measured in an objective and clear manner;
- Feasible: cost-effective to collect;
- Comparable: it should allow comparisons over time;
- Resistant: resistive to manipulation, misuse and misunderstanding;
- Clear: easy to define, report, and evaluate;
- Specific: in relation to what is to be measured;
- Sensitive: reacts to what is being measured;
- Significant: in terms of sample size (number of events);
- Auditable: likely to be auditable.

Some precautions should be taken to prevent manipulation and misuse of performance indicators, especially when using performance indicators in bonus pay systems.
The metrics chosen to establish a quantitative or qualitative SPI system that can be compared to a reference (benchmark) is the main difficulty to be overcome. If an in-house SPI system is used, reference values or qualifications (benchmark)

should be defined by the asset manager, taking into account the objectives set by the management board. However, in the case of an external SPI system, the benchmark should be defined by an independent organisation (e.g. a user group or industry sector association) to enable comparisons between peers.

In addition to the selection criteria, several types of indicators have been proposed.

According to the OECD, indicators can be divided into two types:

- 'activities indicators'; and
- 'outcome indicators'.

Activities indicators are designed to identify whether organisations are taking actions believed to lower operational risks. In contrast, *outcome indicators* are designed to measure whether such actions are, in fact, leading to a lower likelihood of an accident or reducing the potential impact on human health or the environment, should an accident happen (OECD, 2005).

On the other hand, indicators can be divided into two groups, according to their use (Dahlgren, *et al.*, 2001):

- leading (or proactive); and
- lagging (or reactive) indicators.

Leading indicators are useful as a precursor of safety degradation, allowing early management reaction. Lagging indicators are commonly used to drive plant performance, for monitoring, and for benchmarking against similar plants.

Finally, two dimensions of safety indicators can be considered (Hopkins, 2009):

- personal safety indicators versus process safety indicators; and
- lead versus lag indicators.

According to Hopkins, although the distinction between personal and process safety indicators is relatively clear, the distinction between lead and lag indicators, while frequently referred to, is rather more problematic. However, if one is interested in knowing how well safety is being managed, the distinction between lead and lag indicators becomes largely irrelevant, as both will provide relevant information to assess and monitor safety performance.

In summary, besides the great number of definitions that can be found in the literature, what should be kept in mind is the fact that if properly selected, SPIs are useful for:

- evaluating/measuring and comparing safety performance over time for a given asset or group of assets, over a cross-section of assets at a given time, etc.; and
- informing decisions about the safety performance improvement of an industrial asset.

Finally, the selection process of any SPI should consider the effort spent on data collection, treatment and reporting against the usefulness of the information provided, especially in terms of risk-mitigating actions or safety improvement measures that it can generate.

In summary, although performance indicator systems have been established by sector associations to make results comparable between peers, no standardised SPI system has been established so far. Performance indicator systems may provide information regarding the process and equipment safety, but the main objective of such systems is monitoring operational performance and not operational safety.

9.2.2 Maintenance

Maintenance can be managed by different methods according to the type of system or equipment requiring intervention. The simplest method is corrective or run-to-failure maintenance, based on the principle break/repair or replace, which nowadays is seldom applicable to systems or equipment, as usually basic preventive tasks are performed in all of them, such as lubrication, calibration or visual inspection.

Another method is preventive maintenance, where tasks are based on regular time intervals or running hours. This takes into account the specific mean-time-to-failure (MTTF) statistic for each type of equipment, usually available from the manufacturer or in the specialist technical literature. The main disadvantage of this method is that MTTF is an average value that is not kept constant for all similar equipment, which means that either unnecessary maintenance interventions or catastrophic failures can happen. In the first case, labour and material are wasted. However, the second case implies that the run-to-failure method was applied, which is even more costly.

Predictive maintenance is based on a regular monitoring of several operational parameters of the equipment, and process systems will provide the data required to maximise the interval between repairs and minimise the number and cost of unplanned unavailability due to failures. Predictive maintenance is a condition-driven preventive maintenance method. Instead of being based on industrial or equipment average-life statistics (i.e. MTTF) to schedule maintenance activities, it uses direct monitoring of equipment condition, process efficiency and other parameters to estimate the MTTF or loss of efficiency for each system or equipment.

9.2.2.1 Type of Components

Not all equipment and systems have the same importance for the asset manager or the production process. A few of them are so relevant, that a serious failure can produce significant financial losses, resulting from widespread damage and process interruption over a large time period, from several months to one year.

The identification and selection of critical components is generally carried out by dividing the industrial asset components into *critical* and *influence* (non-critical).

A *critical component* can be defined as having the following features:

- its failure can cause an extended forced outage, or
- its failure can endanger the safety of the asset, the environment or personnel, and
- has long lead times and high costs for repair or replacement.

And an *influence component* is characterised by:

- failure results in significant degradation of asset performance but does not cause forced outage, or
- failure does not endanger safety of asset personnel or cause widespread secondary damage, and
- failure susceptibility is known due to 'asset specific' experience.

Examples of critical components in the conventional power generation industry, namely fossil-fired power plants, include live steam piping, turbine and electrical generator rotors and step-up power transformers.

Special attention should be directed towards critical components because the maximum probable losses due to their failures are by far more serious than those from 'influence' component failures. Critical components are the ones where the application of an asset management methodology can reap the most benefits, by avoiding losses due to major accidents.

Bearing in mind this observation, critical components should have clearly defined requirements that are substantiated by records. It is much more advantageous and useful to maintain the strict requirements on a smaller number of items than it is to assign the same criteria to every piece of equipment in the facility (Newslow, 2001). This distinctive feature allows event analyses that can reveal anomalies in systems and the opportunity to enact the necessary preventive measures in good time.

9.2.2.2 Predictive Maintenance

Predictive maintenance is designed to help determine the condition of in-service systems and equipment, and to estimate when maintenance should be performed. This approach enables cost savings over routine or time-based preventive maintenance, because activities are performed only when justified. So, it is regarded as condition-based maintenance, as is carried out in accordance with estimations of the degradation state of a component.

The main advantages of predictive maintenance are to allow convenient scheduling of corrective maintenance, and to prevent unexpected system and equipment failures. In this way, safety foresight is applied in predictive maintenance to define the optimal maintenance period.

In the conventional power generation industry, a critical system, specifically the turbine-generator set, dictates the interval between two power plant maintenance overhauls, as per the manufacturer's instructions. These overhauls are based on running hours and number of starts and allow all the remaining predictive maintenance actions to be adjusted to the turbine-generator overhaul.

9.3 Process Control

According to ISO 9001:2015 Quality Management Systems standard, a *process* is a set of activities that are interrelated or that interact with one another. Processes use resources to transform inputs into outputs and are interconnected, because the output from one process often becomes the input for another process. An effective process control enables a product to be delivered, or service provided to

clients according to the procedures in force at the organisation and hence achieving the required quality standards.

9.3.1 Certification (Quality, OHS, Environmental Management)

In addition to the internal process control in force at the organisation, the quality management system certification provides a universal assessment level. This enables a competent and independent entity—the certification body—to periodically assess the adherence of an organisation's processes to the quality management system principles set out in the ISO 9001 standard. The same is applicable to the occupational health and safety (OHS) management system standard (ISO 45001) as well as to the environmental management system standard (ISO 18001). The certification acts as a guarantee that the organisation is following the requirements established in the relevant standards, and that control mechanisms are set in place to enable the early detection of process degradation. The main advantages of certification claimed by certification bodies include, amongst others, better management control and improved internal communication. Both advantages may have a positive impact on safety foresight.

In addition, industrial companies have physical assets and staff associated with the manufacturing or production process. Usually, in these cases, audits to award or renew the certification include on-site visits to the plants, where areas for improvement can be recommended, including aspects related to process safety. When this happens, safety foresight has been applied.

9.3.2 External Entities

External entities play an important role in establishing rules and controlling organisation activities by reference to directives, regulations, standards, specifications, etc.

Regulators, certification bodies, insurance companies, technologists (high-tech manufacturers), O&M specialist companies, users' groups, and sector associations are a few examples of entities that can help an organisation to be aware of process safety deterioration. In the main, they do this by identifying weak points and recommending preventive and corrective actions to put the process back into conformity with the principles of the relevant reference document or technical specifications.

9.3.2.1 Regulators

Regulators, also known as regulatory agencies, regulatory authorities or regulatory bodies, are public authorities or government agencies responsible for exercising autonomous authority over some areas of economic activity. This includes rulemaking, enforcing rules and regulations, and imposing supervision or oversight for the benefit of the public at large. Some independent regulatory agencies perform investigations or audits, and others may levy fines on the relevant parties and order certain measures to be implemented [see also Chapter 13].

In power generation but also in other industries, there are generally two areas where regulators act to exert their authority: occupational health and safety (OHS) and protection of the environment. The first is a multidisciplinary field concerned with the safety, health, and welfare of people at work. The goals of occupational safety and health programs include providing a safe and healthy work environment. The second deals mainly with environmental pollution control, including air quality, water quality, waste management and contaminant clean up.

Other related areas supervised by regulators include the use of large amounts of dangerous chemicals in industry (under the Seveso Directive), dam structural safety, and emergency safety valves for pressurised equipment used in several process industries that make use of steam in their production processes. In the case of that last example, accredited laboratories calibrate and certify emergency safety valves periodically, according to the regulations set out by the competent authority. If these requirements are not met, the asset owner will have its operating licence cancelled.

So, when major accidents happen, these can pose a significant threat to people and the environment, cause huge economic losses and disrupt sustainable growth; hence the value of external regulation.

9.3.2.2 Certification Bodies

The main roles of certification bodies are to award and issue certificates of compliance with the relevant management system. An auditor is usually involved in the company's certification process (first certification or renewal), by conducting the audit on behalf of the certification body and then by reporting their findings back to it. A consultant can also participate in the process, providing specialist advice to ensure that the management systems will meet the certification requirements.

In the case of OHS, the main advantages of certification to the organisation are to:

- increase employees' awareness and motivation towards safety;
- ensure that official and legal OHS requirements are met;
- prevent accidents;
- reduce downtime and production stoppages;
- reduce the cost of insurance policies;
- improve the organisation's image as a safe and reliable business in the eyes of its clients, suppliers, authorities and investors.

The relevant fact here is that both internal and external audits enable the detection and correction of non-conformities that otherwise would contribute to the occurrence of serious accidents.

9.3.2.3 Insurance Companies

In developed market economies, insurance plays an important role in controlling the risks carried by industrial assets. In simple terms, a company agrees a contract with an insurer to transfer a certain portion of its risk for a determined sum of money, called a *premium*. The contract is called an insurance policy.

Usually, the insurance of large industrial assets is structured so that relatively minor losses are borne solely by the asset holder (Barnard, 2006). This implies that only losses above a certain amount, called the *deductible*, are incurred by the insurance company. On the other hand, the usual practice in the insurance market is also to limit the amount of losses covered by the insurance policy. Both limits, the deductible and the loss coverage of an insurance policy, have a financial impact on the premium paid by the asset holder.

In general, the risk retention and risk transfer strategy depends on the level of risk that a given company is willing to accept and on the premium offered by the insurance market. When the insurance market is *hard* or risk averse—especially following large losses after natural disasters that have generated widespread damage—premiums rise and companies tend to retain a higher level of risk, to keep a similar insurance premium value. When the market is *hard*, two options are available: to increase the insurance deductible or to lower the insurance limit. Increasing the deductible usually reduces the premium more effectively than would lowering the insurance limit. This is because by agreeing a larger deductible, which is the first layer of the insurance policy, the organisation accepts to bear a higher portion of the loss from each accident, up to the deductible limit. Only when the loss exceeds the deductible limit, the insurance policy will cover the remaining portion of the loss.

Usually, high frequency risks result in low severity losses, so these are the risks that will be retained in the company, because usually they fall under the deductible limit. On the contrary, low frequency risks result in high severity accidents, so these are the risks that are typically transferred to the insurance market, as their materialisation could affect heavily the economic activity of the company or even jeopardise its existence as such.

For large industrial companies, there is also the possibility of self-insurance through an internal reinsurance company called a '*captive*', which enables them to retain more risk at an intermediate level of frequency and severity. The mechanism of risk retention and risk transfer is represented schematically in Figure 1.

Figure 1: Risk Retention and Risk Transfer Mechanism (source: Outreville, 1998, p177)

In terms of asset management, the most relevant insurance policy is called *Property Damage.* This type of policy may comprise two parts: *Material*

Damage/Machinery Breakdown (MD/MB), covering losses related to physical assets, and *Loss of Profits* (LP), *Business Interruption* (BI) or *Time Element* (TE), which cover losses derived from the interruption of the company's supply chain. In this context, supply chain means power generation, transmission and distribution, gas supply, pulp and paper production or any other manufacturing process. Only the MD/MB insurance contract can be awarded separately.

However, only sudden, unexpected and random property damage claims are eligible for payment by the insurance companies. This means that equipment failures resulting from wear and tear are ruled out from the insurance contract.

9.3.2.3.1 Audits

In the case of a disaster, the large economic value of industrial assets can impart great financial losses both to asset holders and the insurance companies. Having in mind this possible outcome, insurance companies carry out regular site visits, whose frequency is directly proportional to the total asset insured value (value at risk). Site visits are conducted to check if operational safety is being kept at an acceptable level, according to applicable codes and standards, internal procedures, controls and best practices. Following each site visit, a report can be delivered to the asset holder, mentioning areas for improvement, called recommendations.

9.3.2.3.2 Recommendations

Recommendations are intended to improve the risk and safety of an industrial asset as seen from the perspective of the insurance company. These are based on the global knowledge and experience of the insurance company (statistical data of similar incidents), international standards and insurance company technical datasheets or O&M instructions from critical equipment manufacturers (technologists).

It is well known that insurance companies rely on statistics of previous losses for premium calculation purposes. So, it is not hard to believe that some of the recommendations proposed result from causes related to similar events that have occurred elsewhere, that could not be anticipated and have resulted in a claim. In effect, the goal of an insurance company is to set up a robust asset management system of 'zero accidents'. Although the asset holder pursues the same objective, recommendations involving considerable financial investment should undergo a technical-economic analysis prior to taking the final decision regarding its completion. As financial resources to invest in completion the recommendations are totally incurred by the asset holder, a detailed technical-economic analysis allows to prioritise the ones where major benefits can be achieved at the lowest possible cost.

Typically, the recommendations issued by insurance companies after field visits can be divided into three categories:

- Procedures;
- Inspection and Testing; and
- Systems and Equipment.

This division of insurance recommendations into categories is important mainly for asset management purposes. For example, if most pending recommendations fall into the 'procedures' category, it reveals that the company (the asset holder) has in place an operational safety system with a lot of scope for improvement. In such a case, the insurance company may even request a safety improvement plan, to assure that the company will reach a certain operational safety standard in the shortest time possible. On the other hand, if most of pending recommendations are in the 'systems and equipment' category, it shows a mature operational safety system in place. Under these conditions, and having in mind that operational safety is a continuous improvement process, insurance companies may prioritise those recommendations where, if followed, most benefits can be expected. Although both the insurance company and the asset holder pursue the same objective, which is to reduce operational risk to a satisfactory level, the investment necessary to complete recommendations falls completely onto the asset holder side. Under these circumstances, both will benefit from reducing the probability or consequence (or both simultaneously) of a serious failure, but the asset holder incurs all the costs. In the hypothetical scenario where all the recommendations of this category are implemented, the financial coverage provided by the insurance would decrease so drastically that it would become residual, possibly only useful for 'Act of God' events.

Recommendations relating to procedures ask for new ones to be written or existing ones to be improved, in either case to reach the standards established by the insurance company. However, in a broad sense, procedures have two dimensions. The first is the written procedure itself ('paperwork'), where all the instructions and warnings are laid down. The second is the strict fulfilment of the procedure.

When a procedure deals with inspection and testing instructions, the relevant part is the instructions and then the recommendation falls under the category of 'Inspection and Testing'. When the procedure, as paperwork, needs to be improved or updated, the recommendation is from the 'Procedures' category.

Procedures of the insurance companies address mainly operational safety and fire prevention. Examples include the no smoking policy, 'automatic fire protection systems impairment communication' to the insurance company (for assessing the need of reinsurance), hot work for maintenance works involving flame or heat generation (e.g. oxy-cutting and welding) and contingency plans for critical equipment, typically, generator step-up transformer spare units, for reducing the loss of profits related to the period of unavailability caused by the failure, which can last 12 months or more.

Usually, procedures are not costly in themselves and are easy to set up. However, they may be challenging in some situations because they can present practical difficulties. For example, to check that fire protection systems remain fully operational, emergency procedures require that the systems are regularly discharged. However, as the practical application of procedures are considered under the category of 'Inspection and Testing' recommendations, this will be referred to later.

Usually, procedures are of reduced cost and easy to setup, but may be challenging in some situations, because they can present practical difficulties or be quite expensive to carry out.

Inspection and testing' covers all periodic maintenance actions that are required to keep all safety systems fully operational, and permanently ready for actuation. Generally, recommendations made under this category can be fulfilled at moderate cost. However, in some cases, testing can increase operational risks or become quite expensive to carry out. For example, the overspeed test of a turbine-generator set under actual conditions calls for a 10% increase in rotation above nominal speed. This test creates the risk of serious widespread damage. An example of a costly test is checking the tightness of a turbine enclosure. This requires a full-scale discharge test of its fire protection system: emptying a rack of CO2 gas containers is a quite expensive undertaking. In such cases it is important to reach an agreement with the insurance company to perform the test under electronic simulated conditions or to use an alternative gas for tightness checking of the turbine enclosure respectively.

Finally, systems and equipment installation, replacement, refurbishment or extension entail considerable investment that requires a technical-economic analysis to inform the final decision. Examples include automatic or manual fire protection systems and process safety control devices (e.g. a synchro check relay in the command line of the circuit breaker for synchro in manual mode).

Recommendations issued by insurance companies are one of the most effective tools to continuously improve industrial risk and operational safety. Safety alerts are also used to warn insured asset holders, when property damage has occurred elsewhere in similar equipment. This will enable asset managers to question the technologist regarding the failure risk in its own equipment. In this way, safety foresight is used by insurance companies to prevent accidents in similar equipment elsewhere.

The global knowledge and experience of insurance companies cannot be disregarded as a powerful tool in the prevention of serious industrial accidents. When these accidents happen, insurance companies are called-on to pay the claims, which represent the major part of the property damages incurred. In addition, experts (loss adjusters) are called to perform a thorough accident analysis aiming at determining the root cause and contributing factors of the accident. Once these are determined, insurance companies check if identical conditions are present in similar systems and equipment elsewhere, and if there is a match, recommend preventive actions. In this way, insurance companies use foresight in safety to prevent similar accidents from happening in other locations.

From the side of the asset holder, even if recommendations are not mandatory, and if it is not possible to establish a direct mathematical relation between the insurance premium paid and pending recommendations, it is important for asset managers to make their own judgment about investment priorities in terms of asset risk and safety improvement.

9.3.2.4 Technologists

Technologists, in this context, are specialist firms that have the required knowledge and experience to develop a critical asset, characterised by a highly complex technology manufacturing process, only available to a restricted number of companies. In the power generation industry, gas turbine manufacturers, also called original equipment manufacturers (OEM) for combined-cycle gas turbine (CCGT) power plants is a good example. As only a few exist worldwide, a limited

number of options are available to power generation companies. In addition, the increase in demand for CCGT power plants by power generation companies has raised the competition amongst the gas turbine manufacturers, pushing them to innovate, aiming at reaching higher efficiency rates. Several versions of the same equipment model were released, as manufacturers were introducing improvements constantly, some due to equipment malfunctions or failures in the previous versions. These actions increased the risk of failure, as innovative solutions were released without enough time to mature.

The maintenance of CCGT power plants, particularly gas turbines, is a complex discipline, especially with respect to the integrity of hot gas path components, which is the part of the gas turbine where temperatures can reach as much as 1,200°C. To help asset managers in O&M matters, long term maintenance agreements (LTMA) are offered by turbine manufacturers as a guarantee of specialist technical support, for a period of 15 years or more. Besides maintenance technical support, these agreements may comprise daily event analysis, implying the delivery of all plant operational data to the manufacturer. If process degradation signs are detected, the manufacturer will contact the asset manager for more information about how the equipment is being used or maintained. Finally, when agreed by both parties, LTMA contracts may also include penalties, which can be applied if a pre-set standard quality of service level is not met by the manufacturer.

Once again, the global knowledge and experience of these technologists play a very important role. They are aware of all equipment malfunctions and failures happening globally. When serious failures can jeopardise other similar units elsewhere, a technical information letter is issued and sent to all asset owners of the same equipment version. These technical letters include recommendations about how to operate or when specific parts should be replaced. The rationale is to prevent failures in other similar equipment elsewhere. In this sense, foresight in safety is being put into practice by the cooperative action of the technologist.

9.3.2.5 O&M Specialist Companies

These specialist companies and institutes are usually contracted to carry out specialised industrial tasks using advanced technological means and highly qualified human resources, such as those with expertise on power plant command and control systems and on critical process equipment. In the power generation industry, critical equipment comprises turbines, electric generators and step-up power transformers. These are responsible for the major failures in the power generation industry and the highest value claims paid by the insurance companies. O&M specialist companies have an in-depth knowledge and global experience in the field, which can be very useful when providing O&M specialist services to asset holders. Global experience brings awareness of the major risks and failures involved. An external view by qualified entities is of utmost importance to improve industry processes, procedures and practices.

9.3.2.6 Users' Groups and Sector Associations

Users' groups can be thought of as clubs focused on the use of a specific technology. The groups are usually associated with a company that is a developer or technologist. Although these are external interest groups, the participation of each asset holder allows peers to share relevant information about processes and equipment.

A good example in the power generation industry are the CGGT users' groups that are affiliated with each gas turbine manufacturer. On the CCGT manufacturing technology, the gas turbine is the most critical equipment. Challenged by the electricity market, the power generation industry demanded higher process efficiency rates, fostering a strong competition among gas turbine manufacturers. The rapid evolution of gas turbine technology turned it into a non-mature technology. Failure rates started to increase and company profit losses worsened. Sometimes, failure root-cause analysis carried out by the manufacturers took too long or could not provide satisfactory technical answers to the questions asked by asset managers. Users' groups were the solution found by asset managers to exchange technical information regarding problems encountered in this type of technology. Information about corrective actions that were effective for a specific failure could be shared and applied to similar equipment operated by another user, well in advance or when appropriate. The main objective would be reducing this specific failure probability and improving overall operational safety for all the other users.

Through regular group meetings, formal presentations and attendee-driven discussion sessions focusing on the design, erection, operation, and maintenance of the integrated plant; asset managers are aware of problems and solutions that could be useful to their specific case. In this way, in taking the appropriate

measures, safety foresight is put into practice, as similar potential equipment failures are anticipated and prevented from occurring. This is even more relevant where an LTMA agreement between the asset manager and the technologist is not awarded.

Sector associations act at a higher level than users' groups and deal with a wider range of issues. In the electricity industry, two examples are VGB and Eurelectric.

VGB is the technical association of energy plant operators. Members are companies that operate worldwide facilities for the generation of power, heat and cooling as well as for energy storage and sector coupling. As an independent technical competence centre and network, VGB supports its members in their operational business as well as in the implementation of innovations and strategic challenges. One of the main goals is to strengthen and safeguard a high standard in operational and plant safety as well as health and safety at the workplace. In addition to technical issues, VGB is also actively involved in the political and social debate on technical issues, on behalf of operators. Eurelectric is the sector association representing the common interests of the electricity industry at a European level, plus its affiliates and associates on several other continents. It encompasses all major issues affecting the sector, from generation and markets to distribution networks and customer issues.

As VGB deals with a more specific set of technical issues than Eurelectric, mainly related to the energy plant operators, it is easier to identify potential issues where safety foresight may be applied. VGB provides its members with an international network, a platform for the exchange and transfer of technical know-how, as well as access to qualified expert knowledge via, for example, operational and availability databases for benchmarks. These technical means can be used for a wide range of technical purposes. For safety foresight purposes, the most relevant is the benchmarking tool provided by VGB through power plant performance indicators. However, the indicators available are mainly related to plant performance in terms of availability of power supply to the electrical grid and not to operational safety performance. In this sense, the information obtained through users' groups is more relevant to the daily life of power plant asset managers. This information acquaints asset managers with technical problems that may seriously affect process and equipment safety, allowing them take adequate actions for its prevention.

9.4 Conclusions

Nowadays, industrial assets are managed according to internal procedures, controls, standards and best practices. However, these are also informed by the influence or oversight of external entities, which operate through legal and contractual obligations, or by the asset holder's own initiative. Legal obligations are mandatory, so they cannot be considered an option if the company aims at staying in the market. Contractual obligations can derive from negotiated agreements that require pre-conditions to be set out. If obligations result from the asset holder's own initiative, they are based on the trade-off between benefits derived from the commitments assumed and the incurred costs. In this case, although almost every benefit can be monetised, some of them are difficult to quantify, like the company's image or reputation.

Internal safety requirements like procedures and controls are a very important tool to prevent accidents.

Industrial companies have a set of tools available to monitor process and equipment safety, including proactive and reactive controls, event analysis and performance indicators.

Certification of quality, OHS and environmental management systems are a guarantee that the organisation follows the requirements established in the relevant standards and that control mechanisms are in place to enable the early detection of process degradation. The main advantages of certification claimed by certification bodies include, amongst others, better management control and improved internal communication. Both advantages may have a positive impact on safety foresight.

External entities play an important role in establishing rules and controlling organisation activities by reference to directives, regulations, standards, specifications, etc.

Regulators, certification bodies, insurance companies, technologists (high-tech manufacturers), O&M specialist companies, users' groups and sector associations are examples of external entities that through foresight in safety can contribute to improve the operational risk and safety of industrial assets at different levels. This is particularly true of insurance companies, who are usually the first external entities to be aware, are in close contact with the accidents through loss adjusters, and who have access to confidential, detailed information regarding the causes of

the losses. Inside information of the causes of loss is relevant to similar systems and equipment under operation elsewhere. Under these circumstances, recommendations issued by the insurance company towards improving risk and safety on similar units can be considered as a safety foresight measure.

Finally, asset managers are responsible for the process and equipment safety of the company. They should be aware of all the internal and external tools and entities available to prevent major accidents. By being aware of and using these tools adequately, asset managers can play a relevant role in reducing the probability of major accidents.

9.5 References

Barnard, I. (2006), "Asset Management – An Insurance Perspective", 1st WCEAM - Proceedings of 2006 World Congress on Engineering Asset Management (J. Mathew, J. Kennedy, L. Ma, A. Tan, D. Anderson Editors), 11–14 July 2006.

Chakraborty, S.; Flodin, Y;. Grint, G.; Habermacher, H.; Hallman, A.; Isasia, R.; Karsa, Z.; Khatib-Rahbar, M.; Koeberlein, K.; Matahri, N.; Melendez, E.; Moravcik, I.; Preston, J.; Prohaska, G.; Schwaeger, C.; Tkac, M.; Verduras, E. (2003), "Risk-based Safety Performance Indicators for Nuclear Power Plants", Paper # M01-6, Transactions of the 17th International Conference on Structural Mechanics in Reactor Technology (SMiRT 17) Prague, Czech Republic, August 17 –22, 2003.

Davies, J.; Finlay, M.; McLenaghen, T.; Wilson, D. (2006), "Key risk Indicators – Their Role in Operational Risk Management and Measurement".

Dahlgren, K.; Lederman, L.; Palomo, J.; Szikszai, T. (2001), "Safety Performance Indicators", Topical Issue Paper No. 5, pp. 2, International Conference on Nuclear Safety, Vienna.

Hale, A. (2009), "Why Safety Performance Indicators?", Safety Science 47, pp. 480.

Hopkins, A. (2009), "Thinking about Process Safety Indicators", Safety Science 47 – Special Issue on Process Safety Indicators, pp. 460-465.

Newslow, D.L. (2001), "The ISO 9000 Quality System: Applications in Food and Technology", John Willey & Sons.

OECD (2005), "Guidance on Safety Performance Indicators" (Interim Publication), Series on Chemical Accidents, No. 11, 2003, pp. 8, rev. 2005.

Oktem, U.G.; Seider, W.D.; Soroush, M.; Pariyani, A. (2003), "Improve Process Safety with Near-Miss Analysis", American Institute of Chemical Engineers (AIChE), May 2013.

Outreville J.-F. (1998), Retention, Self-Insurance, Captive Insurance Companies, chapter 10, In book: Theory and Practice of Insurance, Kluwer Academic Publishers, (pp.179-196), accessed on Researchgate, 23rd November 2020

Van Binnebeck, J.J. (2002), "Results of the WGIP Baltimore Workshop Sessions related to PIS", Specialist Meeting on Safety Performance Indicators, Madrid, Spain, 15-17 Oct. 2000, Safety Performance Indicators – Workshop Proceedings, ref. NEA/CSNI/R(2002)2, May 2002.

Van der Lei, T.; Herder, P.; Wijnia Y. (2012), "Asset Management – The State of The Art in Europe from a Life Cycle Perspective", Springer.

This chapter is extracted from the final technical report of the ESReDA Project Group *Foresight in Safety*. The full report is freely downloadable from the ESReDA web site and from the EU Joint Research Centre publications repository.

Bibliographic identifiers for the full report are indicated below.

PDF	ISBN 978-92-76-25189-7	ISSN 1831-9424	doi: 10.2760/814452	KJ-NA-30441-EN-N
Print	ISBN 978-92-76-25188-0	ISSN 1018-5593	doi: 10.2760/382517	KJ-NA-30441-EN-C

How to **cite this report**: ESReDA Project Group Foresight in Safety, *Enhancing Safety: The Challenge of Foresight*, EUR 30441 EN, Publications Office of the European Union, Luxembourg, 2020. ISBN 978-92-76-25189-7, doi: 10.2760/814452, JRC122252.

"Enhancing Safety: The Challenge of Foresight"

Edited by the ESReDA Project Group *Foresight in Safety*.

ESReDA
European Safety, Reliability & Data Association