Demichela Micaela
Dipartimento di Scienza Applicata e Tecnologia, Politecnico di Torino, Torino, Italy

Gallo Mosè
Dipartimento di Ingegneria Chimica dei Materiali e della Produzione Industriale, Università degli Studi di Napoli Federico II, Napol, Italy

Salzano Ernesto
Istituto di Ricerche sulla Combustione, Consiglio Nazionale delle Ricerche, Napoli, Italy

A review of the methodologies for the resilience assessment in the process industry

Keywords

process plants, resilience, risk assessment

Abstract

A widely accepted definition of resilience is the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances so that it can sustain required operational safety under both expected and unexpected conditions. These concepts have been applied in the process or manufacturing industry with different attempts in switching from the traditional risk management approach to a resilience one, still finding a lack of clarity in the definitions and in the objectives and, consequently, a lack in the methodologies and tools to support those efforts. The attempts and the need for further research or clarification is discussed in this paper.

1. Introduction

Resilience assumes different meaning in dependence of the technical or organizational domain. In the most classical significance, it is the physical property that characterises the capacity of any material to return to the original shape or position after deformation that has not exceeded its elastic limits [6]. Following this definition, with regards to the process engineering, Mitchel and Mannan (2006) have given to the term resilience a practical meaning: it is the energy limit of a disturbance that a system can absorb before becoming unstable [10]. In analogy with these definitions, Steen and Aven (2011) [17] have defined the concept of resilience as the probability of a system of succumbing to any negative event, and have formalized it as a function depending on different parameters such as safety barriers, consequences, uncertainty, incidental events. With specific reference to the industrial safety, Pasman and Knegtering (2008) [13] and Pasman et al. (2013) [14] have considered that a resilience approach should be addressed to minimise damages and to restore any system to normal operations immediately after an accident has occurred. Furthermore, they stated that the typical structured analyses for the design and for the management of safety systems are not suitable for the evaluation of industrial risks derived from the combination of different factors as e.g. lack of competence, technical factors, or organization. Hence, a holistic risk assessment is required. Hollnagel et al. (2006) have defined resilience as the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances so that it can sustain required operational safety under both expected and unexpected conditions [7] (see also known and unknown events [11]-[12]).

These concepts have been applied in the process or manufacturing industry with different attempts in switching from the traditional risk management approach to a resilience one, still finding a lack of clarity in the definitions and in the objectives and, consequently, a lack in the methodologies and tools to support those efforts. The attempts will be discussed in the following paragraph. The remaining part of this paper is organized as follows. In paragraph 2 the concepts of risk and resilience are compared. Later, in paragraph 3 and 4 a wider view of the concept of resilience is given discussing the resilience strategies and the relationship between resilience and Safety Management Systems. In paragraph 5 the central theme of risk assessment and resilience assessment is treated. Finally in paragraph 6 some conclusions are presented and an existing research gap is highlighted.

2. Risk vs. Resilience

In the work of Steen & Aven (2011), the concept of “technological risk”, as likelihood of the unwanted events per magnitude of the possible consequence, usually supporting the decision making in major risk premises, has been shifted to a wider perspective based on four parameters: the possible consequences C, the probability P, the uncertainty U, and the background knowledge K, given that the initiating event A takes place.

This set of variable allows representing the resilience of a system, being able to describe the four qualities a system should have to be considered resilient [8]:

i) respond to regular and irregular threats in a robust, yet flexible manner;
ii) to monitor what is going on, including its own performance;
iii) to anticipate risks (risk events) and opportunities; and
iv) to learn from experience.

Since the above variables need a quantification in order to be used for decision making, the methodology that are proposed for the quantification are those traditionally used in risk assessment with the only suggestion of adopting a systemic point of view, thus not taking into account single events, but interrelated ones. It is recognised that the methods based on causal chains and event modelling (like event trees) may produce poor predictions in some cases, but still these methods may provide insights and reveal interesting features of the system. They are also simple and easy to understand, which are attractive properties.

The problem of coping with the uncertainties is not addressed, despite it is recognised to be one of the major criticalities in the risk assessment procedures.

In the paper it is argued that an extended risk assessment supports risk management and ~~the~~ resilience engineering better than isolated processes based on resilience analysis alone. The extended processes ensure a broader perspective, linking the risk with the vulnerability and the resilience and allowing different perspectives to be nurtured.

3. Resilience strategies

As stated in [4] the resilience can be viewed as a kind of forward and pro-active defense. In other words, resilience is the attempt to control the situation by minimizing probability of failure, consequences, and restoration and recovery time.

Through the analysis of the transitions of system states, the multiple factors or measures that characterise the resilience in a chemical process are proposed in *Figure 1*.

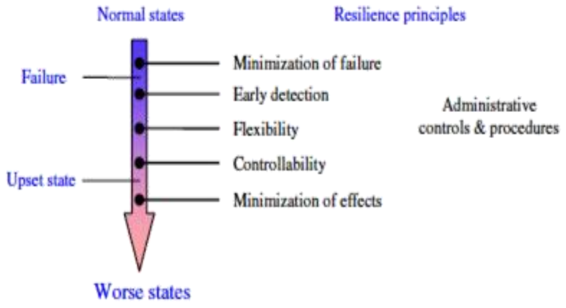

Figure 1. Measures characterising a chemical process resilience [2]

Minimization of failure - is to prevent undesired events from happening by preventive measures. Inherently safer design, proper use of protective equipment, and appropriate safety management should be performed to the maximum extent.

Early detection - When the preventive measures cannot prevent a failure to occur, the role of this principle become evident: no corrective actions can be initiated for failures that remain undetected. In most cases, early response can be achieved by early detection resulting in a more effective response since operators have more time to consider and respond to the urgent situation.

Flexibility - A process is called flexible if output variation can stay in desired range when input is changed due to disturbance within a defined range. This principle thus requires to design a more flexible process that can operate under various disturbances. It is not necessary to return to the previous conditions under disturbance as long as the constraints and specifications are met. Increasing flexibility can help a process not only respond to input fluctuations but also to withstand significant disruptions. Some of common applications of flexibility are to design a plant producing the same product from various types of feedstock, a heat exchange network meeting output temperature specifications when input conditions are changed, and construction materials resistant to various types of corrosion and a wide range of physical conditions.

Controllability - Controllability is the ability of the system to achieve a specific target state It is determined by how effective the system can be controlled, either by feedback or feed-forward methods. A process can be defined controllable if the output parameters to be controlled can be tuned to target points in acceptable time when unexpected input deviates the parameters from the set points. Thus, if flexibility corresponds to steady states, controllability refers to dynamic states and is the ability to reach target points in a certain time. While the Flexibility principle allows processes to operate at various conditions, the Controllability principle allows changing the operation from one condition to another.

Limitation of effects - The more severe the consequences are, the longer it will take for the process to recover. The Limitation of effects principle is to use safeguard or mitigation measures to limit the consequence of an upset event.

Administrative controls and procedures - For certain unexpected disturbances, a solution in the form of a resilient design may be infeasible. Moreover, not every risk can be foreseen by a detection system. Therefore, the resilience principle should involve management systems through Administrative Controls and Procedures. It can affect all the states during the transition from normal to catastrophic states. It is made as early as in design stage and continuously updated in operation stage.

Administrative controls, such as training and standard operating procedures, are another safeguard to prevent and recover from process deviation and accidental release. Training and certification of personnel on critical procedures should be a permanent activity. If operators have the right mental picture of the process and do not panic or neglect alarms, they may even cope with a developing incident by improvising.

4. Safety Management Systems vs. Resilience

Safety Management is an integral part to achieve resilience. Performance measurement through indicators and audits is a core aspect of safety management, it is involved in the mainstream studies related to this area. Costella et al. (2009) devised a method for the assessment of H&S safety management systems, whose requirements were explicitly related to RE premises [2]. A method for assessing health and safety management systems (MAHS) has been described with a resilience engineering perspective on HS, which takes into consideration four major principles (flexibility, learning, awareness, and top management commitment) was explicitated.

Such principles underlie seven major assessment criteria, which, in turn, are divided into items (e.g. hazard identification from a resilience perspective is an item that belongs to the criteria of production processes). The items are sub-divided into statements, which are the requirements that should be assessed based on interviews, analysis of documents and direct observations. Within the 112 requirements proposed, 38 of them have clear links with at least one out of the four resilience engineering principles adopted. The remaining requirements are based on traditional assumptions underlying the so-called best practices of HS management.

As described in literature, the Management Systems needs as a designing support the results of the risk assessment [3], and here the criticalities in the practical application of the resilience growth.

5. Conclusion

It has to be recognised that, with respect to the risk assessment, for the resilience assessment quantitative researches and applications, especially in the process industries, remained relatively undeveloped, as summarised in [15]. In the paper, the authors propose a method for a quantitative assessment of resilience based on six resilience indicators:

i) Top management commitment;
ii) Just and learning culture;
iii) Awareness and opacity;
iv) Preparedness;
v) Flexibility using PCA (principal component analysis); and
vi) Numerical taxonomy (NT) approach.

PCA has the objective to identify linear combinations of the variables that are useful in accounting for the variation in original variables. Numerical taxonomy approach is capable of identifying homogeneous from non-homogeneous cases.

A questionnaire was designed to measure the six indicators. The questionnaire consists of six measuring dimensions: a measure of top management commitment, a measure of Just and learning culture, a measure of awareness and opacity, a measure of preparedness, and a measure of flexibility. The questionnaire included a total of 61 Likert-type questions. Five-point Likert-type scales were utilized in the research, with possible answers ranging from “disagree strongly” to “agree strongly”. The application on the method devised in a process industry, allowed demonstrating that the managers and workers manifested fewer tendencies towards RE approach. However, if the plant decides to be a resilient system, these measurements should be done: (a) creating the reporting system related to accidents, incidents, and near misses; (b) improving the training system itself based on proactive approaches; (c) changing traditional insights (hindsight) about accidents and replacing with foresight; (d) changing accident investigation systems, e.g. seeking for causes of an accident, not hunting scapegoats; (e) considering the safety and resilience as a value; (f) establishing an efficient feedback system in the plant and using its results; and (g) investing for improvement of the safety culture, because it is the backbone for success in the RE programs.

All the measures proposed are, in the end, typical measures that are implemented in safety management systems.

On the other hand the same authors in [16] defined RE as a proactive approach claiming to achieve three main objectives: (a) preventing accidents by anticipation, (b) surviving disturbances by recovery, and (c) handling disruptive events by adaptation; objectives that are not far from the risk assessment’s ones.

The results of this preliminary study, performed through the use of field observation and questionnaires, highlighted qualitatively the challenges in the procedure of building RE and its adaptive capacity in a chemical plant as nine categories: lack of explicit experience about RE, intangibility of RE level, choosing production over safety, lack of reporting systems, ‘religious beliefs’, out-of-date procedures and manuals, poor feedback loop, and economic problems. Working on these aspects the authors argued that it should be possible to achieve an higher level of reliability and resilience in the plant.

This link to reliability is also relevant, because the theory of high reliability organisations (HRO) that is seen as a precursor of the resilience concept – and mostly overlapping with it. HROs are defined in Lekka & Sugden (2011) as organisations that are able to sustain excellent safety records over long time periods, in a ‘‘nearly accident-free’’ manner [9]. These results suggest that there are a number of practices that organisations can adopt to achieve high levels of reliability and safety. These practices are often discussed in the context of major accidents to highlight the safety standards that high hazard organisations should try to emulate. In the cited paper, the reliability-enhancing practices bringing to HRO qualification are explored in a qualitative way in a UK-based oil refinery.

Management commitment to safety emerged as an important factor underpinning the successful implementation of reliability-enhancing practices.

The HRO theory remained unoperalised.

In [5] a system-of-systems framework previously proposed by the same authors for the analysis of the risk of a critical plant (e.g., a nuclear power plant) has been extended to natural external events (e.g., earthquakes). The different parts of the system-of-systems into

i) main inputs, i.e., the infrastructure systems devoted to provide the main supply for the safety of the nuclear power plant;
ii) internal barriers, i.e., the internal emergency devices designed to automatically activate in emergency conditions;
iii) external supports, i.e., the redundant infrastructure systems that can replace the main inputs and the internal barriers when these do not function;
iv) the recovery supporting elements, i.e., the infrastructure systems that can be a support in the actions to keep or restore the safety of the plant have been explicitly modelled.

A multistate model distinguishing structural damage and functional performance of the individual components, that reflects into a multistate model of the system of systems based on different degrees of safety (risk, marginal and healthy) of the nuclear power plant has been built. The system of systems has been represented with a Goal Tree Success Tree–Dynamic Master Logic Diagram (GTST–DMLD) and Monte Carlo simulation has been used for the probabilistic evaluation of the safety of the nuclear power plant and its physical resilience, measured in terms of the time needed to restore the safety. The multistate model was shown to be a valid support for quantify the resilience, provided that the definition of the structural and functional limit states is carefully addressed.

Azadeh et al (2014) proposed a model for the calculation of RE performance indicators with data gathered from a petrochemical plant [1]. Fuzzy cognitive maps have been used for taking into account the interaction between the factors,. Fuzzy cognitive maps (FCMs) are fuzzy-graph structures for representing causal reasoning, as in *Figure 2*. The results showed that preparedness, awareness and flexibility are the most important factor among all nine factor of RE as previously decribed in the previous sections. In addition, redundancy and teamwork play a small role among the RE factors. It is also clear that some factors have almost a similar effect on the resilience of a system that is because of positive causality of the factors on each other. The intended use of the results of this study is to support the managers in determining priorities to allocate the safety assigned to capital.

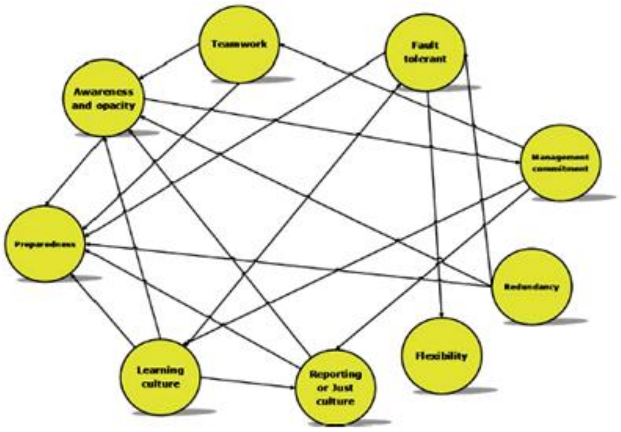

Figure 2. Fuzzy cognitive maps for resilience describing parameters [1]

6. Conclusion

This paper has summarised some experience in the process industry with respect to the operalisation of the resilience theory.

This review has highlighted some basic shortcomings in the application of resilience engineering, and in particular:

i) The set of performance indicators used in RE research (e.g. resilience, robustness, flexibility, adjustments, improvisation, adaptation, stability, variability), need to be revised in order to maximise their operational use and effectivenes, clarifying the aim, the purpose~~d~~ and the final outcomes.

ii) RE need to be placed in in relation to other theories, to which it is strongly interconnected in practice (at least risk analysis and management). The lack of clarity of the conceptual links between RE and the theory of complex systems is also representative of such criticism. For example, lean production shares a number of theoretical assumptions with complexity theory, and it has practices that could be useful for creating an environment that supports resilience

iii) Quantitative methods, such as surveys, mathematical modelling, and computer simulations are not widely diffused, while they are fundamental for decision making.

iv) Rise the need of providing practical guidance to managers on how to design and operate resilient organizations. Thus, there is a need for the development of testable propositions related to RE (e.g. by supporting resilience through the use of a certain practice, under certain conditions, a certain dimension of performance is likely to improve to a certain extent), which can guide iterative cycles of design and evaluation.

References

[1] .Azadeh, A., Salehi, V., Arvan, M. & Dolatkhah, M. (2014). Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: A petrochemical plant. *Safety Science*, 68 99–107

[2] Costella, M.F., Saurin, T.A. & Buarque de Macedo Guimarães, L. (2009). A method for assessing health and safety management systems from the resilience engineering perspective. *Safety Science*, 47, 8, 1056-1067.

[3] Demichela, M. & Piccinini, N. (2006). How the management aspects can affect the results of the QRA. *Journal of Loss Prevention in the Process Industries*, 19, 1, 70-77.

[4] Dinh, L.T.T., Pasman, H., Gao, X. & Mannan, M.S. (2012). Resilience engineering of industrial processes: Principles and contributing factors. *J. Loss Prevent. Proc.* 25, 233-241.

[5] Ferrario, E. & Zio, E. (2014). Assessing nuclear power plant safety and recovery from earthquakes using a system-of-systems approach. *Rel. Eng. & Sys. Safety* 125, 103-116

[6] Garcìa-Serna, J., Perez-Barrigon, L. & Cocero M.J. (2007). New trends for design towards sustainability in chemical engineering: Green engineering. *Chemical Engineering Journal* 133, 7–30.

[7] Hollnagel, E., Woods, D.D. & Leveson, N. (2006). *Resilience Engineering: Concepts and Precepts*. Ashgate Publishing Ltd., Aldershot, UK.

[8] Hollnagel, E. (2007). Resilience engineering. *PSYKOLOGIA* 42 (6), 493.

[9] Lekka, C. & Sugden, C. (2011). The Successes and Challenges of Implementing High Reliability Principles: a Case Study of UK Oil Refinery. *Process Safety and Environmental Protection*, 89(6), 443-451

[10] Mitchell, S.M. & Mannan, M.S. (2006). Designing resilient engineered systems. *Chemical Engineering Progress* 102, 39-45.

[11] Paltrinieri, N., Dechy, N., Salzano, E., Wardman, M. & Cozzani, V. (2012). Lessons learnt from Toulouse and Buncefield disasters: from risk analysis failures to the identification of atypical scenarios through a better knowledge management. *Risk Analysis* 32, 1404-1419.

[12] Paltrinieri, N., Dechy, N., Salzano, E., Wardman, M. & Cozzani, V. (2013). Towards a new approach for the identification of atypical scenarios. *Journal of Risk Reseasech*, 16, 337-354.

[13] Pasman, H.J & Knegtering, B. (2008). Safety of the process industries in the 21st century: A changing need of process safety management for a changing industry. *Journal of Loss Prevention in the Process Industries* 22, 162-168.

[14] Pasman, H.J., Knegtering, B., & Rogers, W.J. (2013). A holistic approach to control process safety risks: Possible ways forward. *Reliability Engineerig & System Safety* 117, 21-29.

[15] Shirali, Gh.A., Mohammadfam, I. & Ebrahimipour, V. (2013). A new method for quantitative assessment of resilience engineering by PCA and NT approach: A case study in a process industry. *Reliability Engineering & System Safety* 119, 2013, 88-94.

[16] Shirali, G.H.A., Motamedzade, M., Mohammadfam, I., Ebrahimipour, V. & Moghimbeigi, A. (2012). Challenges in building resilience engineering (RE) and adaptive capacity: A field study in a chemical plant. *Process Safety and Environmental Protection* 90 83–90.

[17] Steen, R. & Aven, T. (2011). A risk perspective suitable for resilience engineering. *Safety Science* 49, 292–297.