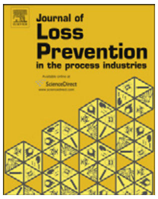
Journal of Loss Prevention in the Process Industries 25 (2012) 233–241

Contents lists available at SciVerse ScienceDirect

Journal of Loss Prevention in the Process Industries

journal homepage: www.elsevier.com/locate/jlp



Resilience engineering of industrial processes: Principles and contributing factors

Linh T.T. Dinh, Hans Pasman, Xiaodan Gao, M. Sam Mannan*

Mary Kay O'Connor Process Safety Center, Artie McFerrin Department of Chemical Engineering, Texas A&M University, College Station, TX 77843-3122, USA

ARTICLE INFO

Article history:
Received 30 March 2011
Received in revised form
12 September 2011
Accepted 13 September 2011

Keywords:
Resilience engineering
Technical failures
Human failures
Random natural events

ABSTRACT

Although many efforts have focused on studying methods to prevent incidents in major hazard plants, mishaps still occur because of various technical and human failures and random natural events. It seems that unexpected disturbances not being absorbed by the system and leading to catastrophes are unavoidable even under good risk management; this seems to be true especially today with the more complex systems. Resilience, which is the ability to recover quickly after an upset, has been recognized as an important characteristic of a complex organization handling hazardous technical operations. In response to the need to further improve the safety of industrial processes or plants, there is a need to study the resilience of a process operation incase unexpected events occur. The aim of this work is to propose the principles and factors that contribute to the resilience of a process. Both are identified based on literature reviews and expert opinions. Six principles, including Flexibility, Controllability, Early Detection, Minimization of Failure, Limitation of Effects, Administrative Controls/Procedures, and five main contributing factors, including Design, Detection Potential, Emergency Response Plan, Human Factor, and Safety Management are identified in this work. An example has been used to demonstrate and support recognized contributing factors. These principles and contributing factors can be applied to evaluations of the resilience of a design or process operation.

1. Introduction of process resilience

In the operation of an industrial process, three system states can be distinguished: normal, upset and catastrophic (Fig. 1). The process systems should be maintained in the normal-state region. However, unwanted disturbances always exist, and tend to force the system state out of the normal-state region. If the system has the ability to detect disturbances and manipulate operating variables accordingly (a function of a process control system), it is likely to stay in the normal state. But the detection may fail, actions may be neglected, and even manipulation may be unable to keep the system state normal. These may cause incidents, such as a product not having proper specifications, small spills, and leaks. As a result, the system state may change to upset. The system can be recovered from an upset to a normal state through effective recovery methods.

If an upset system is not managed properly and is not able to recover to its normal state, then larger events (e.g., massive flammable or toxic material spills, BLEVEs) may follow and the system may cross over into a catastrophic state. This state may still be recovered to normal if action takes place within a certain reaction time. How fast and effective this recovery is will depend not only on recovery plans but also on the system design itself.

Most research in the area of process safety aims to prevent the system state from transitioning downward (the right side of Fig. 1). Increasing effort has been spent on process safety, yet incidents still occur. Those incidents may be caused by technical and human failures and could cause considerable damage to process plants. Moreover, there are always other threats to chemical plants. Some of these include natural causes (e.g., hurricanes) and intentional human acts (e.g., terrorism and sabotage). In large-scale and complex systems, such unexpected situations may occur even if risk management is fully carried out. When these situations occur, minimizing damages and getting operations back to normal are priorities for operators (the left side of Fig. 1). This is the idea of the resilience concept in the industrial processes.

Resilience engineering helps to recover system states after incidents happen rather than prevent incidents from occurring. Incident prevention is a subject of study in other process safety areas (e.g., risk assessment). However, it is impossible to foresee and avoid all threats. Therefore, resilience is needed as an additional safety measure. It should especially be recognized as an important characteristic of the process industry.

Resilience is generally defined as "the ability to bounce back when hit with unexpected demands". Researchers have derived more specific definitions to fit their applications and support their

* Corresponding author. Tel.: +1 979 862 3985; fax: +1 979 458 1493.
E-mail address: mannan@tamu.edu (M.S. Mannan).

0950-4230/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jlp.2011.09.003

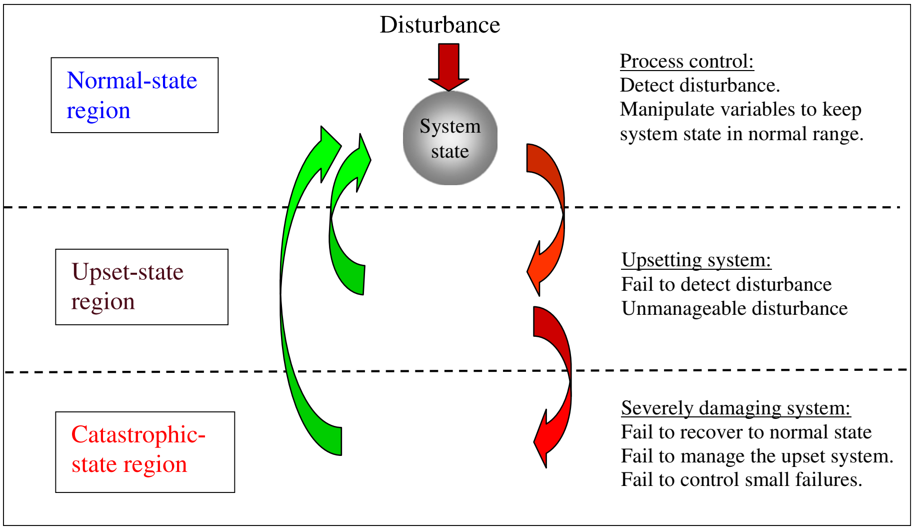

Disturbance
Normal-state region
System state
Process control:
Detect disturbance.
Manipulate variables to keep system state in normal range.
Upset-state region
Upsetting system:
Fail to detect disturbance
Unmanageable disturbance
Catastrophic-state region
Severely damaging system:
Fail to recover to normal state
Fail to manage the upset system.
Fail to control small failures.

Fig. 1. Transition of system state between normal, upset, and catastrophic regions.

quantification approaches. The concept of resilience has been studied for many years in non-chemical disciplines, such as biology, psychology, organizational science, computer science, and ecology. In industrial processes the concept remained relatively undeveloped. Only a few publications closely related to process industry were found.

In management system, Carvalho, Dos Santos, Gomes, and Borges (2008) proposed a qualitative resilience assessment of management system using a micro-incident analysis framework and applied it for nuclear power plant operation. The framework analysis provides an anticipation of the actions that are needed to improve the resilience and safety of organization. Costella, Saurin, and Guimaraes (2008) proposed a new method for assessing health and safety management systems from the resilience engineering perspective. Four major principles of resilience engineering were identified: flexibility, learning, awareness and top management commitment which were used as assessment criteria during the evaluation of health and safety management systems.

In engineered systems, some quantitative methodologies have been developed to assess resilience. Slocum (2007) used experimental disturbances to assess resilience along a known stress gradient. In this work resilience was measured as the recovery rate of the system from a known stress gradient applied. Even though experimental disturbances provide important information about the system and can be used as resilience "probes" by evaluating the recovery rate, it should not be used as a sole evaluation of the stress caused on the system because it also depends on other factors. Mitchell and Mannan (2006) developed a concept of system resilience which was defined as "the amount of energy a system can store before reaching a point of instability". If the input thermodynamic values change, then, the absorbed exergy loads change. The authors borrowed this idea from material science to construct so-called exergy stress and strain curves to track those changes. The curves allow system resilience to be displayed, compared, and qualitatively assessed. The idea was demonstrated in four simple test systems from process engineering, including a steam pipe, water pipe, water pump, and heat exchanger.

Another related research area is flexibility of chemical processes which was developed by Morari et al. in the 1980s and Grossman et al. in 1990s. Morari (1983b) categorized process resilience into two categories based on operation modes: steady state and dynamic state, and treated them in different ways. In the steady state, process resilience was treated as process flexibility (Saboo, Morari, & Woodcock, 1985), i.e. the ability of a plant to handle different feedstock, product specifications, and operating conditions. Saboo et al. (1985) introduced a new resilience index applied to heat exchanger networks to measure the largest disturbance that the network can tolerate without becoming infeasible. The index quantification was then extended by Karafyllis and Kokossis (2002) and Skogestad and Wolff (1996) as a controllability measure to determine the ability of the system to reject disturbances and prevent saturation in the manipulated variables. In the dynamic state, process resilience is simply quantified by the quality level of its control system (Morari, 1983a). Swaney and Grossmann (1982) proposed a resilience measure in a similar spirit. A similar idea is put forward by Saboo et al. (1985) but is specifically related to the resilience (or flexibility) of heat exchanger networks with respect to inlet temperature variations.

In the industrial processes, specifically chemical processes, resilience is the ability to minimize damages and get operations back to normal from adverse events rapidly. The more the resilience of an industrial process is, the lower the consequence is, and the sooner the recovery is. As a result, the risks (which comprises consequence and occurrence frequency) to people, environment and business are decreased. However, the resilience concept has not fully been adopted into the process industry, despite its clear potential benefits related to safety environment, and costs. There seem to be hurdles which limit the application of the concept, and which should be tackled to unveil its potential. The main difficulty in studying resilience is that it is so conceptual. To theorize, manage – even engineer – resilience, it is necessary for basic principles and contributing factors of resilience be identified. The objective of this work is to propose the principles and factors that contribute to the resilience of a chemical process. The following questions will be addressed:

- What are the principal features of positive resilience in a process operation when it is subjected to unexpected events?
- What are the contributing factors that minimize the damages and restore the system?

2. Resilience measures

In an industrial process, at certain conditions even a small disturbance can upset the system, which can then be in a catastrophic state. A resilient system can prevent such highly undesirable transitions through appropriate design, technology, human and management activities and, well planned emergency procedures, which can reverse an incipient mishap and eliminate potential hazardous side effects. Factors or activities which can avoid the transition are called measures (which in terms of risk reduction are called barriers) because they block cause-consequence chains. The importance of the effects of barriers on the safety level have been studied by Haddon (1973), and recently Hollnagel (2004), Hale et al. (2004), Sklet (2006), and Le Coze and Dupré (2006). In the context of resilience, measures will be discussed, because measures can not only stop a development, but also reverse it.

Investigation of transition behavior in the previous section indicates that resilience measures are needed to prevent unwanted transitions and accelerate the desired transition back to a normal state. Coping measures can be pre-installed or even improvised. Fig. 2 shows the effect of resilience measures on the transition of system states. If the measures between disturbance and upset states are effective, the system state goes back to normal. If those measures fail and upset still occurs, there will be protective measures in place that prevent harm to humans and equipment loss. The modeling concept used here is that those measures cannot only prevent loss (as some other process safety measures do) but also help the system to bounce back to a state of normal operation (which is unique to resilience measures). This model also reveals another new concept, resilience, a family of many different measures, not a single one. These different measures work and tie together to improve the ability of the system to tolerate derailing conditions, and to bounce back from disturbances or unexpected events instead of being broken. It is assumed here that the complexity of resilience is derived from the interaction of several simple measures.

3. Strategies and principles of resilience

Resilience can be viewed as a kind of forward and pro-active defense. From the general definition, a resilience strategy can be identified and developed. Resilience strives to control the situation by minimizing probability of failure, consequences, and restoration and recovery time. This can be considered a triple resilience strategy.

To execute the strategy and achieve resilience, the following basic principles are proposed: minimization of failure, early detection, higher flexibility, higher controllability, minimization of effects, and better administrative controls and procedures (ACP). By analyzing the state transition, it can be shown those principles need to be in places and work as layers to perform the resilience strategy (Fig. 3).

To demonstrate how the principles contribute to achieve resilience, a leak of flammable gas is exemplified in the following description of the principle. When a flammable gas is leaked (i.e., process is in failure state), an explosive cloud can be formed. With an ignite source an explosion occurs (i.e., process is in an upset state), which may result in other flame and explosion and cause severe consequences to the process, operators, and environment.

3.1. *Minimization of failure*

Failure is a state that does not meet a desired or intended objective, or which potentially creates a hazardous situation to people (e.g., toxic-gas release) and damage to equipment (e.g., leak, rupture, and suddenly increase of temperature). It is not healthy if safety only depends on operational measures and safeguards or mitigation measures. The Minimization of Failure principle is to prevent something bad from happening by preventive measures.

Inherently safer design, properly using protective equipment, and appropriate safety management should be performed to the maximum extent. In the example, some of preventive measures are choosing gaskets that minimize leak rates of hazardous substances, minimizing stockpiles of toxic substances, exercising careful maintenance (Kletz, 1998), and replacing the flammable gas by a non-flammable one.

3.2. *Early detection*

When the preventive measures cannot prevent a failure to occur, the role of principle Early Detection comes into place. The

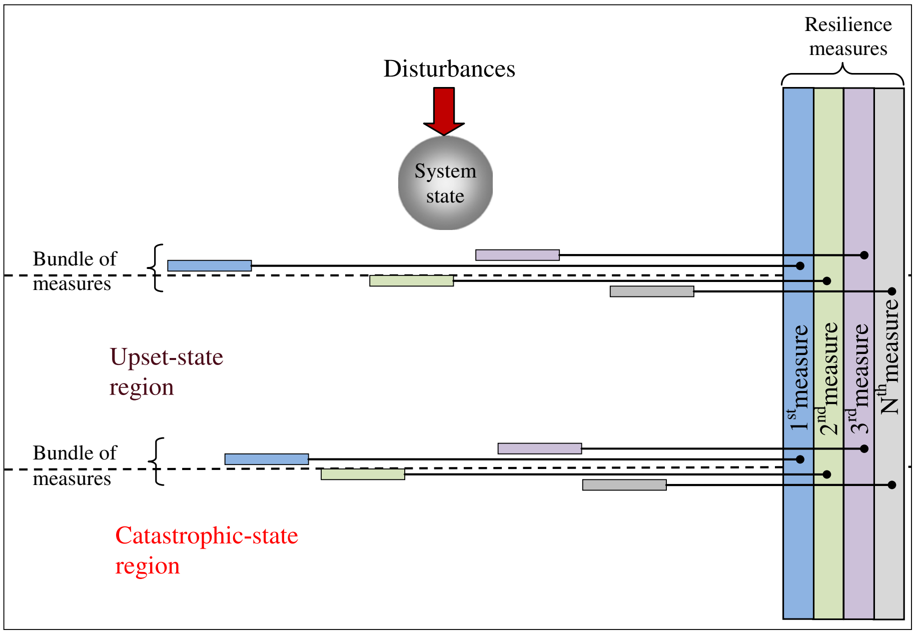


Fig. 2. System bouncing back to normal state with presence of resilience measures.

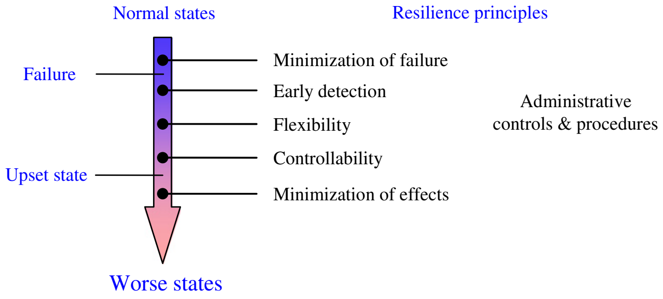


Fig. 3. Resilience principles.

most dangerous disruption and most difficult situation to bounce back from is when disturbance is not detected until it is too late. No corrective actions will be initiated for failures that remain undetected (Van Der Schaaf & Kanse, 2000). Hence, accuracy and early detection is desired for all disturbances. 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.

Many authors (among others, Frese, 1991; Kontogiannis, 1997, 1999; Sellen, 1994; Zapf & Reason, 1994) have clearly stated detection is necessary before the rest of a recovery process can take place. The idea of the detection of the deviation being part of a recovery process was found in the literature (Kanse, 2004). Early detection of a disruption becomes a major determinant of resilience (Sheffi, 2005, 2007). The benefits of early detection in rapid response have also been mentioned in the area of emergency response management system (Kim, Sharman, Rao, & Upadhyaya, 2007).

For the example, the leak should be detected as soon as possible to prevent the gas cloud formation, which may lead to worse situations. The detection is usually made by gas sensors.

3.3. *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 (Fig. 4). The outputs are physical constraints and performance specifications (e.g., target T, P, product specifications).

The Flexibility principle for resilience is 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.

Flexibility was considered as one of the attributes of resilience in previous work of Costella et al. (2008), Sheffi (2007), Saboo et al. (1985), Morari (1983b). Increasing flexibility can help a process not only respond to input fluctuations but also 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.

Refer to the gas leak example, a flexible design will allow to bypass the leaked equipment segment or to reduce gas pressure to minimize leak rate while production is maintained online. Both measures can prevent the hazard situation from escalading to cloud formation.

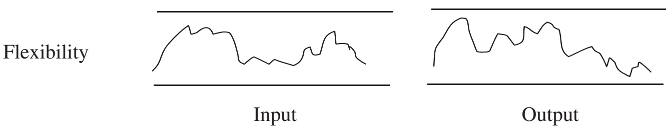


Fig. 4. Flexibility of industrial processes.

3.4. *Controllability*

Controllability is an ability of the system to achieve a specific target state (Rosenbrock, 1970). It is determined by how effective the system can be controlled, either by feedback or feed-forward methods. A process is called 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 (Fig. 5).

Flexibility should be distinguished from controllability. Flexibility corresponds to steady states while controllability refers to dynamic state and is ability to reach target points in a certain time.

The Controllability principle for resilience is to design a more controllable process. While the Flexibility principle allows processes to operate at various conditions, the Controllability principle allows changing the operation from one condition to another. Therefore, both Flexibility and Controllability are needed to achieve the resilience strategy.

Skogestad and Postlethwaite (2005) introduced the term input-output controllability to address the ability to achieve acceptable control performance in which the controlled outputs and manipulated inputs are kept within specified bounds from their set points under any uncertainties. Controllability was also considered as dynamic resilience or as an attribute of resilience in the work of Morari (1983a, 1983b). The better the controllability is, the better the disturbance rejection capacity of the process is (Skogestad & Wolff, 1996).

In the gas leak example, the flexible design allows the process to operate in bypassed or pressure-reduced conditions. However, whether operators can perform the changes and how long to do that depend on controllability of the process. The cloud formation can be stopped only when the new condition is obtained. The sooner is new condition reached, the less is flammable gas released.

3.5. *Limitation of effects*

Despite the low probability of failure, the precise moment when an even may occur cannot be known. If it is not possible to rule out failure or to prevent mishaps, it is important to limit them from becoming worse. 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.

For the example, equipment can be designed in a small volume so that it can leak with only low amount, which would be easy to stop or control. Another measure of the limitation of effects principle can be a building fire wall between sections to restrict the spread of fire. A blast wall to protect control room is necessary in some cases.

3.6. *Administrative controls and procedures*

The upset state or catastrophic state resulting from an unexpected event can be minimized or prevented by design aspects such

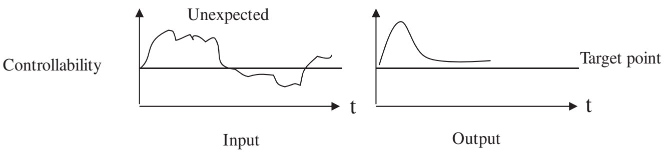


Fig. 5. Controllability of industrial processes.

as flexibility and controllability. However, 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 Kletz (1991). Therefore, the resilience principle should involve management systems through Administrative Controls and Procedures.

The principle is not a layer behind the previous principles. Instead, 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 (Phimister et al., 2003).

In the example, proper maintain procedure can even prevent leak from happening. As other measures, good emergency response plans help to fast stop the leak, isolate the unit, shut down the plant, evacuate the community to minimize the consequences to equipment damage and human loss.

In summary, the resilience definition in the context of industrial processes was used to develop the resilience strategy which in turn is a basis to develop the resilience principles. They are summarized in Fig. 6.

4. Factors that contribute to resilience

It is challenging to implement these principles when evaluating a process for its resilience because there is a lack of systematic attempts to identify factors that contribute to resilience in unexpected situations. Resilience levels of a plant can only be determined if the extent to which factors or attributes that contribute to the resilience of the plant are validated and exercised.

There have been many definitions of organizational resilience and, hence, the associated factors or attributes. Those definitions were found in numerous studies on how organizations dealt with situations that pushed them to the boundaries of competence. Woods (2006) proposed a set of factors which contribute to the resilience developed in prior research, including buffering capacity, flexibility, margin, tolerance, and cross-scale interaction. These factors have been applied in the electric power and telecommunication studies. However, like with other extreme events in chemical engineering, these factors are difficult to evaluate.

In this work, factors or criteria to evaluate the resilience of a process are developed from the resilience principles. The factors must affect the associated principles directly. The major factors that are essential to resilience in global terms are discussed next.

From the Flexibility and Controllability principles of the process, the Design factor is developed. Process resilience is affected very significantly by the design of the process. For example, take the case study in which a batch reactor has a runaway reaction that is caused by the inability of the reactor to cool the accelerating rate of heat produced. If protective measures, such as the use of sufficient pressure relief systems and tanks designed to withstand high pressure and temperature, are in place, then the tank will not rupture or explode, and the system may be back to normal soon after it is cleaned out. Other design features known to increase resilience is increasing the range of heating/cooling capacity to improve flexibility, and fitting the right instrumentation to improve controllability. Several layers of safety systems, whether complementary or redundant, should be considered to enhance resilience as well. For example, in the BP oil spill disaster in the Gulf of Mexico, in the well there was a blowout preventer that was designed to seal off a well in the event of an emergency, but that device had not been working properly since the explosion aboard the Deepwater Horizon oil rig on April 20th 2010 (CNN, 2010).The BP oil spill disaster could have been recovered more quickly if the design would have included a redundancy in which the blowout preventer would perform its ultimate function of closing the well, or had other layers of timely ultimate protection beside this device.

For implementing the principle Early Detection, Detection Potential factor is introduced. Technically, in the runaway example mentioned previously, a special sensor, in combination with a suitable signal-processing device, may warn that a disturbance is emerging before any temperature or pressure deviation is noticeable. However, apart from technical features, here, organizational yardsticks become essential. The quality and implementation of a detection system has the crucial role not only to detect disturbances in time to activate proper safety measures but also, and perhaps even more importantly, to observe the level of resilience improvement or deterioration. Moreover, Detection Systems have also been recognized by Sheffi (2005) as significant elements in building resilience, more specifically for the resilient enterprise through the vigilance concept (Brizon & Wybo, 2006). According to Brizon and Wybo, vigilance is one of the key processes that participate in the resilience of industrial systems. The research of Hollnagel (2006) also agrees with this and mentions “monitoring” as one of the key capacities of resilient engineering. The actions in the process industry to install process safety lagging and leading indicators after the 2005 BP Texas City explosion disaster can be seen as part of this.

A dedicated and well-designed detection system is not enough for a positive resilience. Without the proper management of the

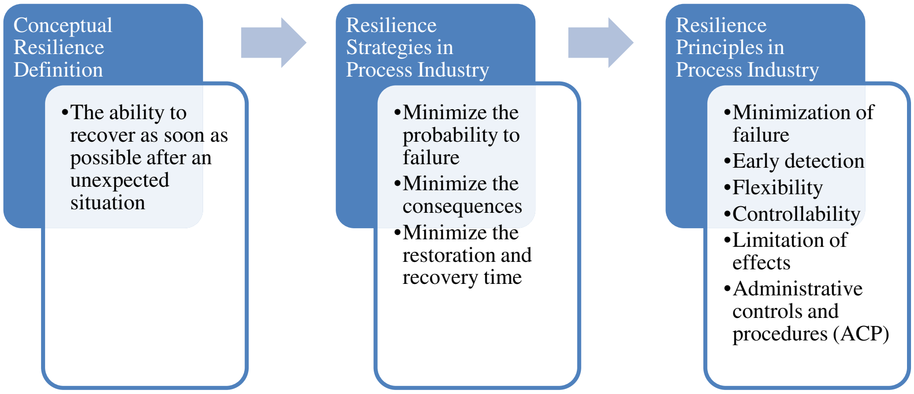

Conceptual Resilience Definition
•The ability to recover as soon as possible after an unexpected situation
Resilience Strategies in Process Industry
•Minimize the probability to failure
•Minimize the consequences
•Minimize the restoration and recovery time
Resilience Principles in Process Industry
•Minimization of failure
•Early detection
•Flexibility
•Controllability
•Limitation of effects
•Administrative controls and procedures (ACP)

Fig. 6. Development of resilience strategies and principles from resilience definition.

alarm system by operations personnel, crucial, quick and accurate detection, assessment and resolution of abnormal operating conditions may not be achieved. The human aspect plays an important role in the response to emergencies and in recovery processes (i.e., the identification and application of appropriate countermeasures) (Kanse, 2004; Van Der Schaaf & Kanse, 2000). Operations personnel missing or misinterpreting alarms can contribute to a more difficult situation for a process to restore and recover from. Operators should be aware of the significance of every stage of the process and the safety procedure to be followed. They should be trained to recognize abnormal conditions or states that may occur. The factor Human also has an important role in detecting the unexpected situation, minimizing the failure and limiting the effects which are the first, second, and fifth principles in Section 3.

The final principle of resilience considers Administrative Controls and Procedures which is involved because carrying out a process under good safety management and good procedures makes the plant more resilient. For example, proper understanding of the process chemistry and thermochemistry by management and adequate operational procedures, including training, can help the plant recover quickly from incidents involving unexpected violent reactions and to prevent more severe consequences. A factor used to evaluate this component of resilience is the Safety Management factor. Employee training is a core aspect of this factor. Operator training supported by process simulation can frequently be improved by showing operators how to respond to upset conditions or process deviations.

Since unexpected situations combine many elements, they are challenging to plan for a respond too. Emergency Response Planning is another important factor that contributes to the characteristic of resilience. The Emergency Response Plan should be well prepared since a rapid and proper response usually results in a shorter recovery time. A situation will be mostly unexpected with regard to time and can be unexpected also with regard to nature. In principle it is impossible to have planned actions in the latter case; however, thorough planning and preparation for the other cases will lay the foundation for a collaborative response. Building joint processes, getting to know all organizations involved in a response, and assigning specific roles are necessary to recover quickly. Moreover, responding – the ability of knowing what to do and being able to do it – was also demonstrated as one of the key capacities of resilient engineering (Hollnagel, 2006). Chemical Safety and Hazard Investigation Board (CSB) has shown that many communities and companies need to be more knowledgeable and better prepared.

Based on the above discussion, it is clear that resilience is the product of many process features covering technical and organizational margins of safety. Five major factors including Design, Detection Potential, Emergency Response Planning (ERP), Human, and Safety Management, have been selected to contribute to resilience in this work (Fig. 7). This means that resilience in major hazard processes can be achieved through better design from a resilience viewpoint, better detection systems, better chemical process safety management, better behavior and quality of employees, and better emergency response procedures. These factors are essential elements in determining response time, and also reflect the fact that intrinsic resilience is affected by many different factors, including the technological, human and management factors. These factors are not sharply defined and tend to intermingle.

These types of resilience factors can be demonstrated in the following example and case study, which support the above selection of the main contributing factors.

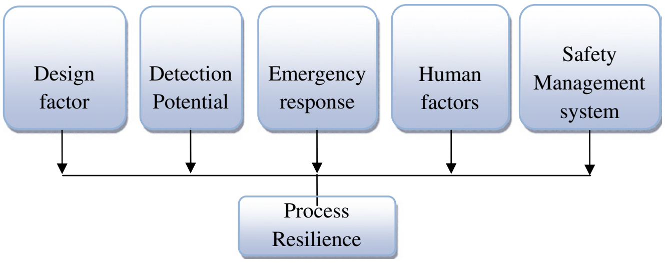


Fig. 7. Contributing factors of process resilience.

Consider a simple example: a leak in a gas-phase heat exchanger (HX). The accident may occur due to a disturbance of the gas flow rate into the heat exchanger. If increased to a certain rate, the gas flow causes acoustic noise and unobserved tube vibration. Later the tube cracks due to prolonged vibration and fatigue. The gas in the high pressure area causes an increase the pressure in the downstream equipment that is connected to the tube side fluid. In the down-stream section, a pipe that was designed to operate at atmospheric pressure cannot withstand the higher pressure, and explodes.

In Design aspect, if the system was designed to eliminate or absorb vibration, then the failure is prevented. Also, if the downstream section of the process was designed to withstand the higher pressure or to have a relief valve, the operator may have enough time to control the gas flow rate back to normal or isolate that HX to replace a new tube or fix the cracks. The recovery time will be faster when the explosion does not occur.

In Detection Potential aspect, if the process was designed with the control system to be able to detect abnormal pressure or temperature profiles due to the leak and control the pipe pressure, then the explosion can be prevented although leak occurred. The HX can be bypassed and process will continue to be in normal operating condition, rather than being shut down due to the explosion.

Human aspect may play a more important role to early detection for the resilience. If the operator can hear the acoustic noise due to vibration in a visual walk and was trained to suspect the vibration, then the HX can be bypassed for inspection and maintenance. Therefore, leak can be even prevented.

With a good ERP, operator is trained to respond to the detected issues by changing the gas flow (when vibration occurs), limiting the pressure increase in the pipe (when leak occurs), safely stopping the blowout flow in the relief valve (when gas is blown out), or closing the gas flow after the explosion.

Safety Management is an integral part to achieve resilience. A regular visual walk may result in the human detection on the acoustic noise. A Hazard and Operability Analysis (HAZOP) conducted in an earlier stage would have indicated where the acoustic noise could potentially come from. Besides, scheduled maintenance activity of the safety management may help to reveal the signs of prolonged vibration in the HX before leak occurs.

If any of those contribution factors are effective, the HX will be back to normal operation quicker without any leak, or with a leak but without an explosion. The system may accept the disturbance (gas flow rate increase), but management can make the HX resilient.

5. Case study

Consider the case where a release of flammable materials leads to an explosion following a runaway reaction and rupture of the reactor as a result of an increase in temperature. It is desired to

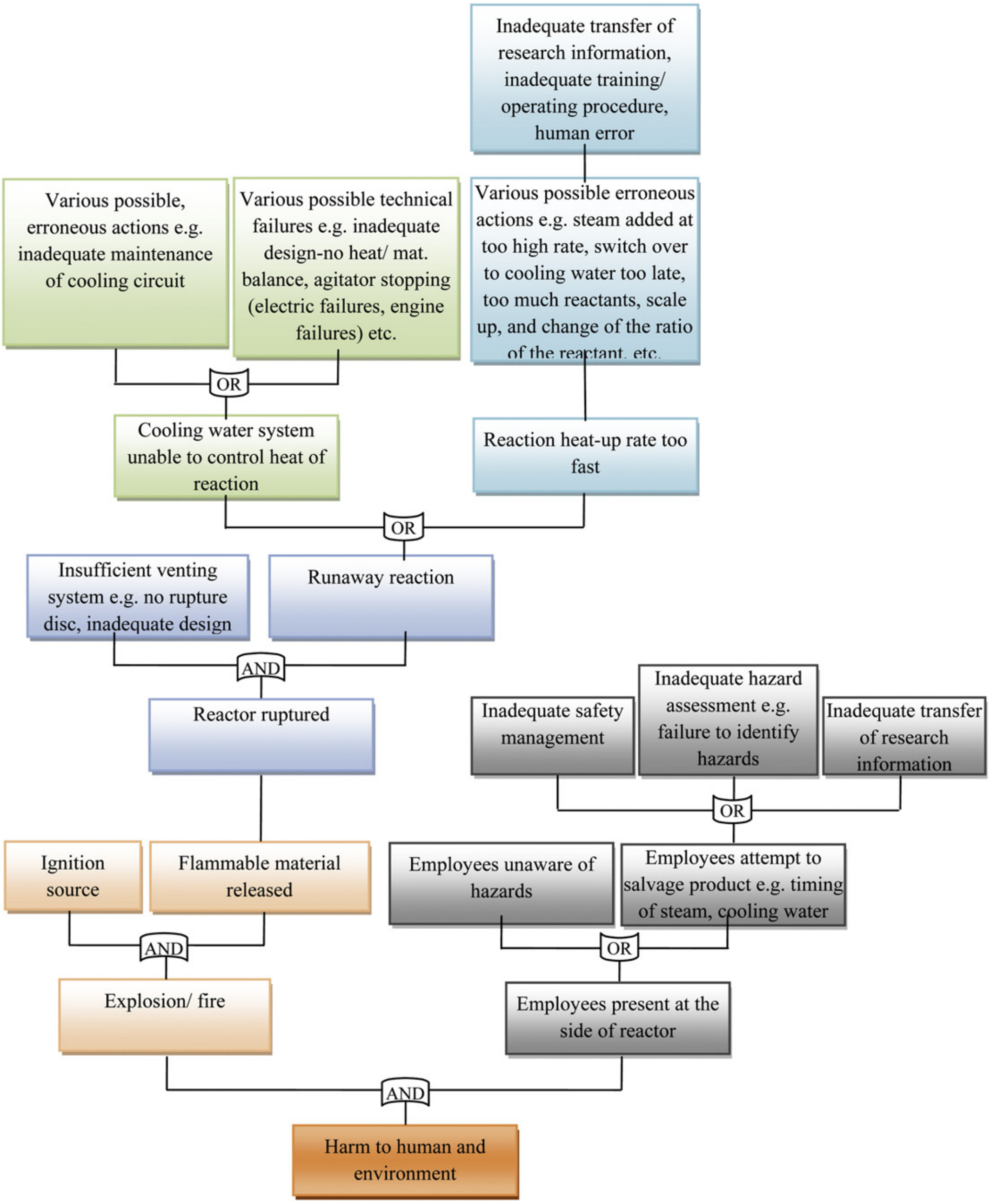

Inadequate transfer of research information, inadequate training/ operating procedure, human error
Various possible, erroneous actions e.g. inadequate maintenance of cooling circuit
Various possible technical failures e.g. inadequate design-no heat/ mat. balance, agitator stopping (electric failures, engine failures) etc.
Various possible erroneous actions e.g. steam added at too high rate, switch over to cooling water too late, too much reactants, scale up, and change of the ratio of the reactant, etc.
OR
Cooling water system unable to control heat of reaction
Reaction heat-up rate too fast
OR
Insufficient venting system e.g. no rupture disc, inadequate design
Runaway reaction
AND
Reactor ruptured
Inadequate safety management
Inadequate hazard assessment e.g. failure to identify hazards
Inadequate transfer of research information
OR
Ignition source
Flammable material released
Employees unaware of hazards
Employees attempt to salvage product e.g. timing of steam, cooling water
AND
OR
Explosion/ fire
Employees present at the side of reactor
AND
Harm to human and environment

Fig. 8. Sequence of the reactor runaway and flammable material release event.

show how the principles and contribution factors can prevent the hazard scenario from developing and assist in getting the system back to normal quicker, meaning the system is more resilient.

To analyze the measures and factors that contribute to resilience, the transition of states is analyzed. The scenario will be considered at different levels of Disturbance, Upset, and Catastrophic consequences. Fig. 8 shows the analyzed results of the state transition which is, in a simple way, the sequence of the events for this example.

Above all, the most effective tool to boost resilience is to prevent something bad from happening, which is based on the fact that there will be no recovery time if no unfortunate incident occurs. In this case study, conditions favorable to possible technical and erroneous failures can be prevented by adequate transferring of research information, hazard assessments, thorough knowledge of the reaction chemistry and thermochemistry, adequate hazard awareness, knowledge of the causes of overpressure, adequate operating procedures, including the order of ingredients, and carefully checked addition rates. Then, depend on a specific scenario, certain measures and factors can be applied to achieve positive resilience for this incident scenario. Those suggested measures and factors are summarized in Table 1.

Analyzing this case study demonstrates that the measures which cut short the chain of undesired events of the case study or contribute to a positive resilience of different scenarios fall into Design, Detection, Emergency Response Plan, Human, or Management categories.

Table 1
Measures, principles, and contribution factors for resilience of the case study.

Disturbance	System state	Measure	Principle	Contribution factors
Erroneous actions such as an incorrect change in the feed ratio, an operator loading too much, loading in the wrong sequence or loading incompatible materials.	Upset: reaction heat-up rate too high.	Design processes, equipment and procedures to neutralize potential human error using inherently safer design e.g. interlocks.	Minimization of failure; ACP	Design; safety management
		Lock software based on values monitored.	Controllability	Design
		Add chemicals to the vessel at a predetermined rate in order to control the rate of the reaction.	Controllability; flexibility	Design
		Issue clear and precise process instruction sheets covering the action to be taken in the event of erroneous actions, e.g., incorrect feeding of reactants, delays in processing, under or over-charging, etc.	ACP	Safety management; ERP
		Operators check product composition in order to recognize abnormal conditions early.	Early detection; ACP	Human; safety management
Technical failures such as inadequate designs involving the heat/material balance, the stopping of agitators due to electric failures and engine failures.	Upset: water-cooling system unable to control the heat of the reaction.	Design adequate heat transfer systems.	Minimization of failure	Design
		Design adequate control and safety back-up systems, e.g., a software action linked with heat excess alarms in case of power loss, agitator failure, and coolant failure.	Controllability; minimization of failure; early detection	Design; detection potential
		Operators recognize abnormal conditions and perform proper actions.	Early detection; ACP	Human; ERP; safety management
		Issue clear and precise process instruction for abnormal conditions, e.g., loss of agitation, loss of cooling water.	ACP	Safety management; ERP
Water-cooling system unable to control the heat of the reaction or the reaction heat rate is up too high.	Upset: runaway reaction.	Fit a high temperature indicator and alarm system (e.g., high pressure alarm) to the vessel in give early warnings of potential runaway.	Early detection	Detection potential
		Use smart signal processing to recognize abnormal temperature or pressure conditions.		
		Cut off the feed and heating from vessel when a predetermined maximum safe temperature or rate of temperature rise is reached.	Controllability	Design; ERP
		Add chemicals to cancel the effects of the catalyst.	Limitation of effects	Design; ERP
		Neutralize, quench with water or other diluents, or dump the contents into a vessel which contains a quench liquid programmed to be activated at a high pressure threshold.		
		Issue clear and precise instructions for the operators to follow.	ACP	Safety management
Runaway reaction.	Catastrophic: reactor ruptured/exploded.	Provide sufficient relief systems, such as a suitable vents and bursting disc/relief valves to be used when the safe working pressure of the vessel is exceeded.	Minimization of failure	Design
		Use a tank designed to withstand high pressures and temperatures.	Flexibility	Design
		Recognize abnormal conditions and execute appropriate actions.	Early detection; ACP	Human; ERP; safety management
Reactor ruptured.	Catastrophic: flammable material released.	Design a suitable catch pot that can collect what is released and withstand the pressure of the discharge from the reaction vessel.	Limitation of effects	Design
		Use a vent scrubber that is designed for treating atmospheric emissions in cases of high pressure in any catch tank that requires the release of products into the environment.	Limitation of effects	Design
Flammable material released.	Catastrophic: fire/explosion.	Area and equipment are classified to prevent ignition sources.	Limitation of effects	Design
		Reduce ignition probability by ignition source control by restricted access and permit to work (PTW) system.	ACP	Safety management
		Install a device, e.g., a water spray, to rapidly cool the space above the reactor, so the hot reaction products do not self-ignite after mixing with air and generate a secondary vapor cloud explosion.	Limitation of effects	Design
		Emergency Response Actions by operation, deluge, water spray, and fire brigade.	ACP	ERP
Fire/explosion	Catastrophic: harm to people.	Keep the number of people in the vicinity of the reactor to a minimum.	Limitation of effects; ACP	Safety management

6. Conclusion

This work discussed the importance of considering resilience characteristic in the chemical process, an undeveloped research area. The aim of this work is to develop new principles and contributing factors that constitute resilience of a chemical processes.

Analyzing transitions of system states revealed that resilience is characterized by multiple factors or measures. These measures work and interact together to improve the ability of chemical processes to bounce back. The principles of resilience were proposed to be Flexibility, Controllability, Early Detection, Minimization of Failure, Limitation of Effects, and Administrative Controls/ Procedures. These principles act as guidelines to help develop the multiple contribution factors for numerically evaluating resilience. The first-layer of factors that contribute to resilience was proposed to be Design Factor, Detection Potential Factor, Emergency Response Factor, Human Factor, and Safety Management Factor.

The application of this work is to develop a system to evaluate the resilience of a chemical design, process, or plant based on the "multi-level, multi-attribute" approach.

References

Brizon, A., & Wybo, J. L. (2006). Vigilance: a process contributing to the resilience of organizations. In *Proceedings of the second resilience engineering symposium*, France.

Carvalho, P. V. R., Dos Santos, I. L., Gomes, J. O., & Borges, M. R. S. (2008). Micro incident analysis framework to assess safety and resilience in the operation of safe critical systems: a case study in a nuclear power plant. *Journal of Loss Prevention in the Process Industries, 21*, 277–286.

CNN. (2010). BP document: worst-case scenario – 4.2 million gallons daily in Gulf. http://www.cnn.com/2010/US/06/20/gulf.oil.disaster/index.html?hpt=T1 Accessed on 20.06.10.

Costella, M. F., Saurin, T. A., & Guimaraes, L. B. M. (2008). A method for assessing health and safety management systems from the resilience engineering perspective. *Safety Science*, .

Frese, M. (1991). Error management or error prevention: two strategies to deal with errors in software design. *Human aspects in computing: Design and use of interactive systems and work with terminals* (pp. 776–782).

Haddon, W. (1973). Energy damage and the ten countermeasure strategies. *The Journal of the Human Factors and Ergonomics Society, 15*, 355–366.

Hale, A., Goossens, L. H. J., Ale, B. J. M., Bellamy, L. A., Post, J., & Papazoglou, I. A. (2004). Managing safety barriers and controls at the workplace. In C. Spitzer, U. Schmocker, & V. N. Dang (Eds.), *Probabilistic safety assessment & management* (pp. 608–613). Berlin: Springer.

Hollnagel, E. (2004). *Barriers and accident prevention*. Hampshire: Ashgate Publishing.

Hollnagel, E. (2006). Resilience: the challenge of the unstable. In E. Hollnagel, D. Woods, & N. Levenson (Eds.), *Resilience engineering* (pp. 9–19). Aldershot: Ashgate Publishing.

Kanse, L. L. (2004). Recovery uncovered: how people in the chemical process industry recover from failures.

Karafyllis, I., & Kokossis, A. (2002). On a new measure for the integration of process design and control: the disturbance resiliency index. *Chemical Engineering Science, 57*, 873–886.

Kim, J. K., Sharman, R., Rao, H. R., & Upadhyaya, S. (2007). Efficiency of critical incident management systems: instrument development and validation. *Decision Support Systems, 44*, 235–250.

Kletz, T. (1991). Inherently safer plants: an update. *Plant/Operations Progress, 10*, 81–84.

Kletz, T. (1998). *Process plants: A handbook for inherently safer design*. Philadelphia: Taylor & Francis.

Kontogiannis, T. (1997). A framework for the analysis of cognitive reliability in complex systems: a recovery centred approach. *Reliability Engineering & System Safety, 58*, 233–248.

Kontogiannis, T. (1999). User strategies in recovering from errors in man-machine systems. *Safety Science, 32*, 49–68.

Le Coze, J. C., & Dupré, M. (2006). How to prevent a normal accident in a high reliable organisation: the art of resilience, a case study in the chemical industry. In *Proceedings of the second resilience engineering symposium*, France (pp. 8–10).

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

Morari, M. (1983a). Design of resilient processing plants – III. A general framework for the assessment of dynamic resilience. *Chemical Engineering Science, 38*, 1881–1891.

Morari, M. (1983b). Flexibility and resiliency of process systems. *Computer Chemical Engineering, 7*, 423–437.

Phimister, J. R., Oktem, U., Kleindorfer, P. R., & Kunreuther, H. (2003). Near miss incident management in the chemical process industry. *Risk Analysis, 23*, 445–459.

Rosenbrock, H. (1970). *State-space and multivariable theory*. London.

Saboo, A. K., Morari, M., & Woodcock, D. C. (1985). Design of resilient processing plants – VIII. A resilience index for heat exchanger networks. *Chemical Engineering Science, 40*, 1553–1565.

Sellen, A. J. (1994). Detection of everyday errors. *Applied Psychology, 43*, 475–498.

Sheffi, Y. (2005). Detecting disruptions. In *The resilient enterprise: Overcoming vulnerability for competitive advantage* (pp. 155–171). The MIT Press.

Sheffi, Y. (2007). Building a resilient organization. *The Bridge-The Journal of National Academy of Engineering, 37*, 30.

Sklet, S. (2006). Safety barriers: definition, classification, and performance. *Journal of Loss Prevention in the Process Industries, 19*, 494–506.

Skogestad, S., & Postlethwaite, I. (2005). *Multivariable feedback control: Analysis and design* (2nd ed.). West Sussex: John Wiley & Sons.

Skogestad, S., & Wolff, E. A. (1996). Controllability measures for disturbance rejection. *Modeling Identification and Control, 17*, 167–182.

Slocum, M. G. (2007). Use of experimental disturbances to assess resilience along a known stress gradient. *Ecological Indicators, 8*, 181–190.

Swaney, R. E., & Grossmann, I. E. (1982). A metric for operational flexibility in chemical process design. In *AIChE annual meeting*, Los Angeles, CA.

Van Der Schaaf, T., & Kanse, L. (2000). Errors and error recovery. *Human Error and System Design and Management, 253*, 27–38.

Woods, D. D. (2006). Essential characteristics of resilience. In E. Hollnagel, D. D. Woods, & N. Levenson (Eds.), *Resilience engineering* (pp. 21–34). Hampshire: Ashgate Publishing.

Zapf, D., & Reason, J. T. (1994). Introduction: human errors and error handling. *Applied Psychology, 43*, 427–432.