Development of a Resilience Model for the Analysis of Process Systems at the Early Design Stage

Freya Vesey[1,2] and Joan Cordiner[1]

[1]Department of Chemical & Biological Engineering, The University of Sheffield, Sheffield S1 3JD, UK
[2]Cavendish Nuclear, 106 Dalton Ave, Birchwood, Risley, Warrington WA3 6YD

Resilience addresses a system's ability to survive significant and unexpected deviations and then recover. Hence, a resilience approach to the assessment of a system's response to beyond design basis events is a valuable concept in process design. Resilience is now a widely discussed concept yet no methodology has been agreed to comprehend and quantify resilient performance, limiting its application. There is a need for an analysis framework that is relevant and applicable to a wide variety of systems, introducing a standardized analysis for the measurement and comparison of resilience. This paper details the development of a novel and accessible model for the assessment and scaling of process system resilience from the early design stage, a period when the opportunity to introduce resilience into a system is high. The model combines analyses of resilient design with susceptibility to high-impact events, providing the opportunity to determine if further investment toward resilience would be beneficial. This model consists of 3 sections: 1) an index-based quantification of resilient design (in turn giving design consequences for improved resilience), 2) potential for severe human health, economic and environmental impacts due to beyond design basis events, 3) vulnerability to beyond design basis events. From applying this model, it is clear that traditional design methodologies do not extend well to give a resilient effect; proving the need for specified resilience analysis. The analysis has also allowed for cost-benefit assessment for design improvements towards resilience. This model presents an effective, useful, and necessary tool for the introduction of resilience as a design concept that, with some further development, can be used widely throughout industry.

`Keywords: Resilience, Beyond Design Basis, Design Stage Assessment

1 Introduction

Resilience is a relatively new process safety concept, extensively discussed in recent years. Traditional hazard analysis studies risk as a function of the combined probability and consequence of a hazard. In contrast, resilience is a 'what if?' analysis that considers how a system will deal with the impact of a hazard by its ability to withstand disruption, avoid catastrophic failure, then recover. This is a valuable concept for consideration of severe and unexpected events such as natural disasters and terrorist attacks which may not be adequately addressed with traditional hazard analysis studies. Resilience is therefore presented as a non-probabilistic, worst-case scenario study, a concept that should be considered in addition to existing risk studies; particularly useful in high hazard environments.

However, due to the recent introduction of the term, the explicit definition of resilience has not yet been agreed upon and the understanding and practical application of the concept is in its infancy. Furthermore, many existing approaches offered for resilience analysis of process systems are arduous and complex, meaning resilience analysis is currently a lengthy and inaccessible task for many organisations to complete. As no widely accepted and practical approach for this has been developed the concept is currently difficult to apply, with organisations required to create their own methodology for its measurement. This is seriously limiting the industrial application of this important concept. A standardized approach to resilience analysis must therefore be developed which offers a simple and clear methodology, allows for the comparison between systems, and can be adopted across the process industry.

This paper aims to define resilience, helping to create a framework to develop an accessible and straightforward numerical analysis of the concept, necessary for the standardized analysis of resilience throughout industry. The developed model is applicable across the process industry and is capable of assessing resilience from the early design stage to both guide design and encourage operation with resilience as a focus. This will allow for resilience to be built into a system as a fundamental pillar.

2 The Importance of a Resilience Approach to Process Safety

Safety analysis methods employed in the process industry overwhelmingly take a risk analysis approach where risk is taken as a function of the severity of a hazard and the likelihood that the hazard will occur. Risk-based approaches will then award actions to reduce a hazard's impact or to implement barriers blocking the hazard from affecting a system. This is an important approach but relies on the assumption that hazards and their impacts can be predicted and effectively mitigated which may not always be possible without unreasonable cost. (Azadeh et al., 2014) If a hazard were to impact a system there is often little consideration for how it would react post-event. (Pitblado, et al., 2016) Hence, risk analysis is not an appropriate strategy to address high severity/low-frequency hazards which cannot be realistically predicted or prevented e.g., natural disasters. A further limitation of taking risk as a function of both severity and likelihood is that the low frequency of unexpected events is used to justify lower levels of mitigation for this hazard. If a severe yet unexpected hazard does occur, the system will not be adequately protected against and its impacts will be catastrophic. These high severity hazards should be considered in process safety analysis, regardless of their likelihood.

Furthermore, the accuracy of risk predictions with the use of past data is inherently limited and often misleading, particularly for low-frequency events with little past data available describing these. Commonly many assumptions must be made and uncertainties are often not adequately considered. (MacAskill, 2021) Our ability to identify and address these inaccuracies is low, resulting in low-frequency, high-hazard events being repeatedly underestimated and hence inadequately mitigated against in a risk analysis approach. Furthermore, the total number of possible hazards which may affect a system is theoretically endless. Therefore, in addition to inaccurate prediction of known hazards, inevitably many hazards will be completely unexpected and won't be considered during a hazard analysis.

The limitations of risk analysis mean that the following scenarios could significantly impact a system in the event of their occurrence:

1. High impact hazards that can't be completely protected against
2. High impact hazards, receiving inadequate consideration due to their low-frequency
3. Underestimated or unexpected hazards

These hazards inadequately addressed by traditional safety analysis are termed beyond design basis events (BDBEs). These are severe and unexpected hazards including events of the scale of natural disasters and terrorist attacks. This shows that in addition to risk analysis, it is crucial to introduce a resilience approach to safety to address how a process system will react to and cope with the impact of these extreme events, regardless of their likelihood. Subject to disturbance, a resilient system can withstand variation, absorb a portion of the impact, and recover in a timely manner. (Gilbert, 2010) This gives a system with reduced failure probability and reduced overall consequences/losses when impacted by extreme events.

The justification of investment to improve process resilience is complicated as, if a BDBE does occur, the potential health, environmental and economic consequences will be disastrous, yet this is not foreseeable in a plant's lifetime. Hence return on investments are unlikely to be observed meaning they should be prioritised towards areas with high effectiveness and low cost. Additionally, only the most severe of scenarios can reasonably be considered for resilience investment meaning many lower hazard industries may not require resilience consideration and just a conventional risk analysis approach will suffice.

3 Applying a Resilience Approach

Process safety resilience is still in its development with no universally agreed definition beyond its general concept and no widely accepted framework existing for its measurement. With little practical understanding of the term, along with a drive to save costs and a tendency for normalcy bias, resilience is commonly implemented insufficiently. (Orosz et al., 2020) Hence, to push resilience to become a widely understood and considered concept throughout industry there is a demand for an accessible, standardized, and widely applicable model for its quantification. A broad framework that is relevant to and easily applied across many process sectors is required.

3.1 Limitations to Common Resilience Quantification Techniques

An extensive literature review has been conducted to assess current resilience analysis models. Many of these rely on the detailed dynamic simulation of system responses to specific disruptions and data from these responses used via varying equations to give resilience. (Yodo and Wang, 2016) This is not appropriate for the intended analysis for multiple reasons.

Firstly, detailed system modelling is challenging to complete in the design stages as a high degree of detail is needed, requiring extensive system knowledge. (Azadeh et al., 2014) In many cases, despite detailed models being developed, significant assumptions are required to apply these, often nullifying the intricacies of the model. (Francis and Bekera, 2014) For the described reasons, the reliance on detailed system modelling should be avoided.

Additionally, using individual simulations regarding each potential BDBE is not a practical framework for resilience analysis as all feasible events must be considered. This would require a vast number of simulations creating a very demanding, lengthy, and technically specialised process, not easily available to most organisations. Furthermore, there will inevitably be failure modes that have not been predicted during the design stage, further limiting the effectiveness of this approach. (Orosz et al., 2020)

Finally, existing resilience quantification approaches give no indication of how system characteristics relate to resilience. This means further expertise are required to implement resilience improvements, further limiting the accessibility of these approaches. Instead, a methodology must be focused on the industrial application of resilience, providing a practical viewpoint of resilience and leading to clear design consequences of resilience improvements for organisations to act upon.

3.2 A New Approach to Resilience

In response to the review noted above, the novel approach taken will differ from existing individual hazard simulation approaches to provide a more accessible methodology, encouraging ease of application in practical engineering settings. This will be completed by:

- Avoiding reliance on complex system modelling
- Giving a single, holistic value of resilience for a process system broadly describing its resilience to a wide range of BDBEs

- Giving an indication of the system properties of which resilience is a function, hence pointing to pathways for resilience improvement

With these objectives, a resilience model has been developed with the aim of being clear and effective whilst increasing understanding of this complex concept; encouraging the standardized consideration of resilience throughout industry. This methodology is capable of measuring resilience by the human health, economic, and environmental impacts of a BDBE and is a broad analysis with the aim of assessing a wide range of the potential BDBEs that may impact a system. Additionally, this analysis is intended to be straight forward so can be easily carried out by the competencies available to a project; presenting a methodology that is accessible to all organisations.

4 Model Framework

4.1 Model scope

The developed model will be suitable for use throughout a range of sectors including chemicals, manufacturing, food & drink, pharmaceuticals, and, water. This resilience analysis considers hazards with a relatively short time from initiation to the point where the most severe consequence is suffered, giving little time to respond. In contrast, BDBEs such as pandemics can be foreseen relatively early and the response planned to give a controlled and safe shutdown, hence won't be addressed in this analysis. Finally, attention should be drawn to the nature of this model which broadly comprehends resilience, providing an effective snapshot for design stage assessment.

4.2 Introduction to The Model Framework

As discussed, only systems with the potential for severe hazards should be considered for resilience investment. Therefore, the analysis of resilient design must be supported by the analysis of the necessity for resilience of a particular process system; a function of the hazard posed by the system. This will inform an organisation if resilience improvements are necessary.

To assess the extent to which resilience of design is warranted, the severity of consequences due to an extreme event is measured with potential impact analysis, describing the potential human health, economic and environmental threat posed by a system. Then, to assess system susceptibility to uncontrolled hazards, vulnerability analysis is completed. This expresses the risk that a system will suffer serious consequences to an initial event, enabling severe impact to a system. Vulnerability analysis is completed by considering the propagation of hazards through a system, triggered by an initiating event. These components have been combined in a novel framework to give the overall system resilience, Ψ, as:

$$\Psi = \frac{Resilient\ Design}{Potential\ Impact\ .Vulnerability} \qquad (4.1)$$

This assessment should be used to measure resilience starting in the early design stages and used iteratively throughout design as updated information is made available and factors of resilience become more relevant for consideration. This will ensure that resilience remains a fundamental philosophy of design as the system develops as well as ensuring investments towards resilience remain effective and justified.

4.3 Resilient Design

Defining Resilience

To quantify resilience the term must first be clearly defined. As resilience describes a process system's ability to both survive significant disruption with minimal consequences and then recover, the concept is seen to be a function of two distinct characteristics or dimensions of resilience; 'survivability' and 'recoverability' as described below. (Yodo and Wang, 2016) The use of these dimensions gives an appropriately broad definition to develop a framework around whilst allowing for the detailed consideration of factors within each dimension.

- **Survivability**: Survivability captures an engineering system's ability to minimise the severity of impact due to a disruption. (Taleb-Berrouane and Khan, 2019)
- **Recoverability**: Recoverability captures an engineering system's ability to undergo corrective actions to recover from disrupted operation. (El-Halwagi et al., 2020)

The Use of Metrics to Describe Resilience

To define the specific system properties which can be used to quantify resilience, there must first be a consideration of the system qualities that influence survivability and recoverability, referred to as metrics of resilience. A collection of metrics will be used to describe each dimension, effectively capturing the many elements which contribute to resilience. Many metrics exist in literature which have been reviewed and the necessary collection to effectively describe resilience have been presented below.

Metrics of the Dimension of Survivability:

- **Early Warning** – Disturbance detection is required before mitigating and remediating actions can be taken. Early detection and a good understanding of a disruption allows for quick implementation of these actions. (Dinh et al., 2012)
- **Robustness** – Robustness denotes the given level of stress that a system can withstand without consequences to performance. (Bruneau and Reinhorn, 2007)
- **Absorptive Capacity** – Absorptive capacity describes the portion of the impact of a given disruption that the system can neutralise or absorb. This mitigates the stress a system is put under, resulting in decreased consequences. (Francis and Bekera, 2014)
- **Flexibility** – Flexibility describes a system's ability to acceptably operate over a wide range of process conditions due to error-tolerant design. (Dimitriadis and Pistikopoulos, 1995) The term can also be seen as the dampening ability of a process to operate normally, maintaining output specifications, despite disruption. (Dinh et al., 2012)

Metrics of the Dimension of Recoverability:

- **Resourcefulness** – A system's level of recoverability depends on the resources available to it and the system's ability to mobilise these resources quickly. (Yodo and Wang, 2016)
- **Controllability** – Controllability describes the ability to direct and steer a system from a dynamic and disrupted state to a recovered equilibrium state. (El-Halwagi et al., 2020)
- **Reconfigurability** – Supporting resourcefulness, reconfigurability describes the ability of a system to smoothly transition to and operate with different configurations to reinstate safe operation. (El-Halwagi et al., 2020)

Development of Indicators of Resilient Design

Each metric should be described and quantified by specific and measurable system properties, indicators of resilient design, as shown in figure 4.1. Indicators clearly display the properties that make a system resilient allowing for its analysis, comparison between systems, and measurable improvement; something that has not yet been clearly defined. Indicators are developed with the philosophy of broad applicability to ensure the model is relevant to a wide variety of process systems. Furthermore, each indicator gives an independent pathway to improved resilience meaning any combination can be altered to give a flexible strategy for improvement.

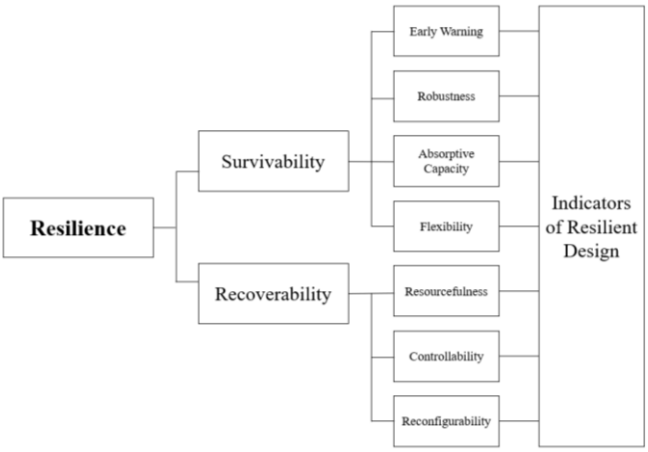

Figure 4.1 - Resilience Described by its Dimensions, Metrics and Indicators

In addition to engineering design, human factors can have a significant impact on the resilience of a system. This is because effective resilient action by system design only is often not feasible when presented with extreme events and human intervention is often necessary. (Dinh et al., 2012) This has been reflected in the indicators shown which fall into two categories; technical and administrative factors. This stresses the need for consideration of resilience from the early design stages through to operation and indicators should be considered as and when they are relevant.

All indicators proposed are quantified with a range of 0 to 1, with higher values denoting a more resilient system. Indicators are determined by simple calculated fractions, rating scales, or binary yes/no questions; each requiring only easily obtainable data to be gathered. Each indicator is weighted to reflect its overall contribution to resilient design. Those relevant to multiple metrics will be weighted to reflect this contribution through numerous pathways. As an indicator's contribution to resilience is subjective, weighting is completed through the use of a questionnaire distributed to experts in process safety.

27 indicators of resilient design have been presented in tables 4.1 and 4.2. It is seen that there are significantly fewer indicators of recoverability which is expected as this describes the aftermath of an incident, hence is more challenging to consider in the design stages and is the less understood of the two dimensions. (Yodo and Wang, 2016) This collection of indicators can be seen as a starting point, and system properties providing resilience may be added or removed in future revisions of the model as resilience is further explored and understood. Finally, there may be dependencies between some indicators when applying them practically. Therefore, whilst making improvements to resilient design checks should be completed to ensure resilience is not sacrificed unduly in other areas.

Table 4.1 – Indicators of the Dimension of Survivability

Metric	Indicator	Summary
Early Warning	Diversity of Monitoring	The measurement of multiple parameters to assess overall system health allowing for reliable and better-informed identification of disruptions.
	Duplication of Monitoring	The use of multiple sensors to measure a single system parameter, ensuring reliable system monitoring.
	Operator Knowledge	Operators should be knowledgeable of the process they are working with and be capable of recognising adverse conditions quickly as they develop.
Robustness	Safety Margin	High safety margin describes the use of components with higher than typical error tolerance to give increased system robustness. (Yodo and Wang, 2016)
	Reliability - Equipment Design	Equipment reliability under normal operation is highly impacted by the equipment design. This is important as failure in conjunction with external disruptions, or the simultaneous failure of equipment can result in a BDBE. (Hewitt and Collier, 2018)
	Reliability - Predictive maintenance	Failed or degraded equipment will again leave a system vulnerable to further hazards. Predictive maintenance pre-empts this to avoid or mitigate potential disruptions.
	Reactive Maintenance	Reactive maintenance must be timely and to a high standard to minimize equipment downtime and ensure full reinstation of mechanical integrity.
	Management of Change	Standardized procedures to ensure communication between relevant parties upon a change in procedure mitigates unexpected internal disruptions.
Absorptive Capacity	Operator Knowledge	Operators should be knowledgeable of the process and be able to action relevant emergency procedures accurately and quickly. (Dinh et al.2012)
	Administrative Knowledge	Human intervention may be required to mitigate the impacts of a disruption. Appropriate technical staff should be available at all times to complete this.
	Segregation of Equipment	The potential for cascade failure is dependent on the physical availability of items of equipment to each other. Therefore, segregation (via distance and physical barriers) is advantageous for survivability.
	Layers of Safety Systems	Safety systems are necessary to mitigate failure consequences and avoid failure propagation. For units with multiple safety systems, each should be independent and diverse.
	Design of Safety Systems	Passive safety systems are preferred over active systems as have reduced vulnerability to component failure and human error.
	Emergency Procedures	Emergency procedures must be in place with regular training and review to ensure they can be effectively deployed when needed. (Jain et al., 2018)
	Tests of Safety Systems	Safety systems should not only be maintained but also be regularly tested to ensure they are fit for purpose. (Jain et al., 2018)
	Diversity of Emergency Services	A system subject to an extreme hazard will often be reliant on external emergency services for survivability. Multiple providers having access to a facility mitigates a lack of availability when these services are required.
	Fail-Safe Design	A resilient system should be capable of suffering component failure in a safe manner that avoids failure propagation.
Flexibility	Redundancy of Safety-Critical Utilities	For reliable delivery of safety-critical utilities during operation or controlled shutdown a system must have alternate utility sources available to it if the original source fails. (Yodo and Wang, 2016)
	Modularity of Unit Operations	Failure of a smaller, modular unit will have decreased consequences due to the lower volume of hazardous materials which may be released. Additionally, there is potential for production to continue at decreased capacity using unaffected units. (Dinh et al., 2012)
	Modularity of Facilities	Spreading operation across multiple sites, significantly geographically separated, encourages the avoidance of an entire system being impacted by a single hazard and for operation to be continued at a decreased capacity using unaffected sites.

Table 4.2 – Indicators of the Dimension of Recoverability

Metric	Indicator	Summary
Resourcefulness	Modularity of Unit Operations	Production can be continued or increased through unaffected units whilst a failed unit is repaired. Additionally, small modular equipment can be manufactured and transported quickly, allowing for fast repairs.
	Modularity of Facility	Modularity of facilities gives the ability to continue or increase production at unaffected sites to make up for that lost at impacted sites.
	Administrative Knowledge	Human intervention may be required to remediate system disruptions. Appropriate technical staff should be available at all times to complete this.
	Throughput Adaptability	The ability to safely increase throughput across unaffected units supports equipment and facility modularity. Additionally, after a period of shutdown increasing throughput allows for a system to make up for production loss.

Controllability	Response to Control Measures	A system's response to safety measures made by the control system dictates its ability to regain control and move away from unsafe conditions quickly.
Reconfigurability	Redundancy	Redundancy involves the use of 'stand by' equipment that can replace failed equipment, moving the system back to normal operation.
	Reconfigurability of Flowsheet	Altering the flowsheet during dynamic operation supports other recovery capabilities e.g., deploying redundant equipment and bypassing failed equipment. This task should be simple, fast, and elegant to complete.

Cost-Benefit Analysis

When improving resilient design through any of the 27 indicators presented only the most effective and low-cost improvements should be implemented. Therefore, consideration of relative effectiveness through a cost-benefit analysis is imperative. An investment priority weighting is introduced which is multiplied by the contribution to resilience weighting. This gives a cost-benefit rating for each indicator. Indicators scoring highly are seen as most favourable for investment towards resilience improvements. A questionnaire is again used for investment priority weighting, to be completed by the particular organisation adopting this model, giving a customised cost-benefit analysis.

4.4 Potential Impact

Potential impact is considered for human health, economic and environmental impacts. To maintain model simplicity the completed analysis is deterministic to assess the wide range of possible hazards and their consequences within each of these categories. Hence, a system's worst-case scenario is assessed where all existing safety systems are assumed to have no effect. As this method is not dependent on highly specific hazards and their effects, the use of the model across a wide range of process systems is straightforward. Furthermore, as many different hazards will have a similar impact on a system, this simplified approach will deliver a similar level of accuracy. This model comprehends potential for impact through two general groups; potential for economic impact and potential for impact on human health and the environment.

Potential for Economic Impact

Potential for economic impact is taken as a function of potential damage to the facility and loss of production (e.g due to loss of plant functionality or necessary plant quarantines) leading to loss of revenue. Potential damage to the facility is quantified by the system's capital cost, assuming a BDBE may have the capability to destroy an entire facility however appreciates that this will not always occur. Capital cost is used as a standardized and easily found value, giving a good proxy measure of the potential economic impact due to damage to the facility. To describe the economic impact due to loss of production the yearly revenue is used. This assumes a BDBE may have the capability to halt production for a year but appreciates that production may be impacted for any amount of time. Again, this offers a standardized and easily found value giving a snapshot of this quality. Therefore, the potential for economic impact is described by equation 4.2 where CC is the capital cost ($) and R is the yearly revenue ($/year).

$$Potential\ for\ economic\ impact\ = CC + R \quad (4.2)$$

Potential for Impact to Human Health and the Environment

The potential impact to human health and the environment is composed of 3 main sections: Chemical Hazard Potential, the Human Health Impact Rating, and the Environmental Impact Rating. The separate assessment of these offers for the individual comprehension of each factor before they are combined to give the overall potential impact.

Chemical Hazard Potential

To assess the potential for impact to human health and the environment it is important to consider the chemical inventory present on a plant (including stored quantities) and the physical states in which they are present. The hazards associated with each material is measured by the Chemical Hazard Potential (CHP), an industrially accepted concept used to reflect physio-chemical, toxic, and environmental hazards. The calculation of CHP for a system is taken from the approach used by the Nuclear Decommissioning Authority (NDA) which utilizes Control of Major Accident Hazard (COMAH) limits. (Nuclear Decommissioning Authority, 2011). Equation 4.3 shows the calculation of CHP where FF_M is the form factor (modified for this application), CF is the control factor, and Clnv is the COMAH inventory, calculated for each chemical present at a facility, k. If a material exists in multiple phases, then the CHP of each phase must be calculated due to the different form factors and potentially different hazards associated with each phase.

$$CHP = \sum_k CHP_k = \sum_k \frac{Clnv_k . FF_{M,k}}{CF_k} \quad (4.3)$$

The phase of materials dictates the potential for loss of containment as this will control the ease that they can migrate into the environment where they can contaminate surroundings and be exposed to adverse conditions e.g., flammable material being exposed to an ignition source. Additionally, the phase of a material dictates the range and rate at which it can travel when containment is lost. These characteristics are described by the form factor (FF_M), which has been modified from the form factor values used by the NDA. This is to reflect a liquid's increased potential for loss of containment and increased rate and range of movement once containment is lost, compared to less mobile sludges and solids. FF_M values are shown in table 4.3. Furthermore, the control factor (CF), shown in table 4.4, describes the length of time which a material will be left on site without monitoring or intervention, reflecting the opportunity for loss of containment.

The COMAH inventory for each chemical, k, ($Clnv_k$) is calculated by equation 4.4. Here, m_k is the mass of chemical k in tonnes and c_k is its COMAH limit (found using COSHH databanks). For a batch or semi-batch system where the materials present on site are variable, it is suggested to calculate CHP for the maximum volume of a given chemical present at any time during operation. This takes a worst-case scenario approach, in line with the resilience concept, where the maximum amount of hazardous materials is assumed to exist at a facility in conjunction

$$Clnv_k = 10^{11} \frac{m_k}{c_k} \qquad (4.4)$$

Table 4.3: Modified Form Factor, FF_M (Nuclear Decommissioning Authority, 2011)

Phase	FF_M
Gas	1×10^{0}
Liquid	5×10^{-1}
Sludge	1×10^{-1}
Powders	1×10^{-1}
Discrete solids	1×10^{-5}
Large monolithic and activated compounds	1×10^{-6}

Table 4.4: Control Factor, CF (Nuclear Decommissioning Authority, 2011)

Time material is left without monitoring or intervention	CF
Hours or less	1×10^{0}
Days	1×10^{1}
Weeks	1×10^{2}
Months	1×10^{3}
Years	1×10^{4}
Decades	1×10^{5}

Table 4.5 – Environmental Impact Rating Assigned to the KBA Scale (KeyBiodiversityAreas.org, 2022)

KBA Colour Scale	Environmental Impact Rating, E
	1×10^{1}
	1×10^{2}
	1×10^{3}
	1×10^{4}
	1×10^{5}
	1×10^{6}
	1×10^{7}

Human Health Impact Rating

The system's CHP must then be put into the context of its surroundings to properly describe the scale of potential consequences to human health. This can be described by considering the population surrounding the facility with the human health impact rating, H. To describe the correlation between the severity of consequence and distance from the facility, this population has been split into two general groups. The first is the critical population, P_c; those close to the impact region who are under the highest risk in the event of system catastrophe and are most likely to be directly impacted (e.g., fire, explosion, and toxic release). The second is the wider population, P_w; those susceptible to impact, yet likely to a significantly lower severity such as failure of infrastructure (e.g., loss of electricity and damage to buildings), and impacts to mental health.

The critical population is taken as the largest number of personnel on-site during normal operation, including staff in adjoining offices. Any further population which may be directly impacted by an extreme event, such as those inhabiting directly around a facility, should also be accounted for here. To find the wider population it is assumed that the consequences of a severe hazard can impact an area up to 10 km from the plant. (IAEA, 2022) Therefore, the population residing within this radius is taken as the wider population. When combining these two groups to give the human health impact rating, the increased magnitude of potential impact to the critical population is reflected by weighting this value appropriately. This is shown in equation 4.5 where an index of 5 is used which also ensures H is appropriately sensitive to this lower value of P_c compared to P_w.

$$H = P_c^5 + P_w \qquad (4.5)$$

Environmental Impact Rating

To assess the impact that an extreme event can have on the environment it is again important to consider the surroundings of the facility. To do this, the environmental impact rating, E, is used which considers the plant's proximity to ecosystems that would suffer due to a process disaster. Impact to a richer ecosystem would result in more severe environmental consequences, therefore, the health of a system's surrounding environment must be measured.

Biodiversity is an effective descriptor of environmental health and therefore the potential environmental impact. This is measured for an area of 10 km radius around the plant. Data is used from the group 'Key Biodiversity Areas' which collects data for Key Biodiversity Areas (KBAs) globally. This data can be found as a discrete colour scale plotted on a global map, to which an E rating has been assigned, as shown in table 4.5, with a higher E denoting a richer environment.

Potential Impact – Final Equation Form

The human health and environmental impact ratings can then be combined with the CHP to give the overall potential for impact to human health and the environment. This is shown in equation 4.6. From equations 4.2 and 4.6 the final equation form describing the potential for economic, human health, and environmental impact is shown as equation 4.7. To further develop this analysis, it is recommended to incorporate a measure of the potential impact of legal implications and impact to a company's reputation due to the occurrence of a major accident.

$$Potential\ impact\ to\ human\ health\ and\ the\ environment = CHP(H + E) \qquad (4.6)$$

$$Potential\ Impact = (CC + R) + CHP(H + E) \qquad (4.7)$$

4.5 Vulnerability

Vulnerability analysis is also completed through a deterministic approach independent of the initiating event and instead, the worst-case scenario consequences are studied. To quantify system vulnerability to severe events cascade failure is considered which would enable a system to suffer uncontrolled consequences of an initial impact. Hence, a system with a high risk of cascade failure will be highly vulnerable to severe and unexpected events.

Combustible substances are particularly susceptible to cascade failure, making up 89% of substances involved in cascade failure events. (Darbra et al., 2010) Therefore, vulnerability to uncontrolled events is quantified by the mass of flammable and explosive material present on a plant. Vulnerability is considered without regard for the safety systems and procedures in place to mitigate against fire and explosions to consider a worst-case scenario event. CHP analysis is modified to express system vulnerability to each of the two major initiating modes of fire and explosion which are: (Crowl and Louvar, n.d.)

- The ignition of flammable or explosive substances (including dust)
- Explosion due to excess pressure exerted by gasses causing the mechanical failure of the containment vessel

Vulnerability to Fire and Explosion due to Ignition

Using a modified form of equations 4.3 and 4.4, the CHP due to ignition (CHP_i) can be found to quantify the vulnerability of a system to this failure mode. The COMAH inventory of each flammable and explosive chemical present on a process plant, l, ($Clnv_l$) is found by using the COMAH limit with respect to flammability and/or explosion hazards only (c_l). This is shown in equations 4.8 and 4.9. The remaining requirements for fire or explosion, oxygen, and heat/ignition sources, aren't specifically considered in this analysis. This is because these elements are assumed to be readily abundant in and around a plant as atmospheric oxygen is always available and ignition sources are difficult to exclude in an industrial setting.

$$Clnv_l = 10^{11} \frac{m_l}{c_l} \qquad (4.8)$$

$$CHP_i = \sum_l CHP_{i,l} = \sum_l \frac{Clnv_{i,l} . FF_{M,l}}{CF_l} \qquad (4.9)$$

Vulnerability to Explosion due to Excess Pressure

For the consideration of vulnerability due to excess pressure, an assumption is made to simplify the analysis that this event would only occur due to the heating of gas and that this uncontrolled heating will only occur due to a runaway exothermic reaction. This is a common initiator of explosions of this nature with 167 serious accidents involving runaway reactions occurring between 1980 and 2001. (Crowl and Louvar, n.d.)

When considering uncontrolled heating of gasses upon a runaway reaction, a process that exerts heat at a slower rate will have a longer time before an explosion occurs. With more time for intervention to control a process, where safety features can be put to use more effectively, a system will be less vulnerable to explosion. Therefore, it is useful to introduce a term describing this dependency on the speed of heat production. For an exothermic reaction, r, the heat of reaction (Q_r), giving the energy expelled per mole reacted, effectively describes the rate of heat production. It should be noted that no speed factor is used for vulnerability due to ignition as this occurs instantaneously when fuel is exposed to ignition sources in oxygen.

To describe this quality, the CHP of explosion due to excess pressure (CHP_p) is found for all gaseous materials susceptible to a runaway reaction i.e., those held in a vessel accommodating an exothermic reaction, m. These vessels, and the material held in them, must be identified and the risk of explosion due to gas being heated used to find the COMAH limit for all relevant material with respect to this hazard only (hence c_m = 150). COMAH inventory with respect to explosion due to excess pressure ($Clnv_m$) and CHP_p is then found using a modified form of equations 4.3 and 4.4.

$$Clnv_m = 10^{11} \frac{m_m}{c_m} \qquad (4.10)$$

$$CHP_p = \sum_m CHP_{p,m} = \sum_m \frac{Clnv_m \, FF_{M,m}}{CF_m} . \; Q_r \qquad (4.11)$$

Vulnerability – Final Equation Form

The final equation describing vulnerability to uncontrolled events is the simple addition of equations 4.9 and 4.11.

$$Vulnerability = CHP_i + CHP_p \qquad (4.12)$$

4.6 Resilience - Final Equation Form

Now resilient design, potential impact, and vulnerability have been described, equation 4.1 can be updated to give overall system resilience as shown in equation 4.13. System resilience should be calculated from the early design stages and updated as new information is made available. The results should be used to influence design throughout all stages and through to operation, guided by indicators of resilient design.

$$\Psi = \frac{\Sigma \, n_j i_j}{[(CC + R) + CHP(H + E)] \; [CHP_i + CHP_p]} \qquad (4.13)$$

where

Ψ	Resilience,	CHP	Chemical Hazard Potential,
n_j	Contribution weighting of indicator j,	H	Human health impact rating,
i_j	Resilience of design with respect to indicator j,	E	Environmental impact rating,
CC	Capital cost, $,	CHP_i	Chemical Hazard Potential due to ignition,
R	Annual revenue, $/year,	CHP_p	Chemical Hazard Potential due to excess pressure, kJ/mol.

5 Project Results

This methodology has been trialled on two process designs at a similar point in their design stage.

5.1 Indicators of Resilient Design – Results of the Contribution and Cost Analysis

Questionnaires to find the weighting of indicators with respect to contribution to resilient design and investment priority were distributed to an industry expert. Investment priority was weighted for a non-specific process system for the purposes of these trial simulations. From the analysis of contribution ratings, it is seen that all indicators have a significant contribution to resilience. With a scale of 0 to 10 (with 10 denoting high contribution), the average rating was 7.6, with a range from 3 to 10. Cost-benefit ratings have an initial scale from 0 to 100 (with 100 denoting the most favourable indicators for investment), however, since some indicators are relevant to multiple metrics of resilience, their cost-benefit ratings are added. Therefore, the average cost-benefit rating was 74, ranging from 25 to 200. The potentially large benefit to resilience by investing in indicators contributing to multiple metrics of resilience is clearly displayed as the indicators receiving the highest cost-benefit ratings are:

1. Operator knowledge (contributing to the metrics of early warning and absorptive capacity)
2. Modularity of Facility (contributing to the metrics of flexibility and resourcefulness)

5.2 Case Study Results

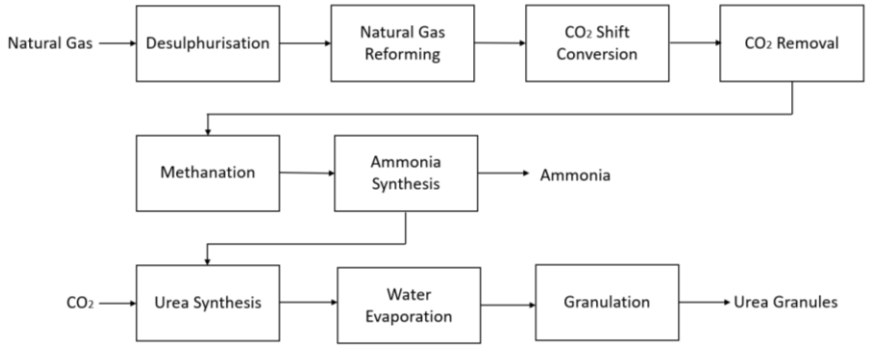

Figure 5.1 –Block Flow Diagram of an Ammonia and Urea Production Process (Scattergood et al., 2020)

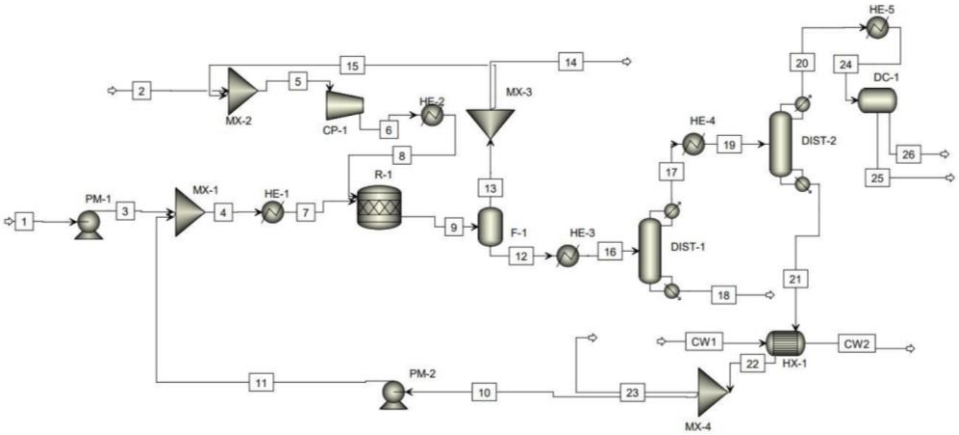

Figure 5.2 – PFD of a p-Aminophenol Production Process (Ghoroi et al., 2021)

Case study 1 is an ammonia and urea production process based in Houston, Texas, and produces 300,000 tonnes of ammonia and 280,000 tonnes of urea per year. (Scattergood et al., 2020) Here hydrogen is sourced from the processing of natural gas. The system predominantly handles gases however liquids and solids are also processed. This process design provides a good level of information to complete a resilience analysis with as a class 4 cost estimation, Hazard Identification Study (HAZID), Layers of Protection Analysis (LOPA), and plant layout are available. The BFD of this process is shown in figure 5.1.

Case study 2 is a p-Aminophenol production process designed by Ghoroi et al. (2021). This presents a facility based in India, producing 22,000 tonnes of p-Aminophenol per year via the reaction of nitrobenzene with hydrogen gas; also producing aniline as a side-product. For this reaction, hydrogen is used as a feedstock and the system predominantly handles liquid

however gas is also processed. This system design included cost analysis and some basic safety considerations however some detail was missing for this resilience analysis. Therefore, some assumptions were made including placing the site centrally in one of India's major industrial regions, the Mumbai-Pune Industrial Area, and assuming an industry-standard site layout. Furthermore, a number of systems and procedures given by indicators of resilient design are not addressed by the available information (significantly due to the lack of safety analysis e.g., HAZID). The affected indicators are assumed not to be considered by this design, hence score low. It should also be noted that this system holds around 7 times the mass of material on-site at any one time compared to case study 1. The PFD describing this system is shown in figure 5.2.

After applying the developed model to these case studies, the results are reviewed and the model iteratively adjusted to ensure good sensitivity to all factors considered. To do this, coefficients have been assigned to components of resilience, giving equation 5.1. The model has been scaled around two of the 3 dimensional values considered, capital cost (CC) and annual revenue (R), as these give a good base to scale resilience around. It should be noted that this model doesn't give mathematical continuity with respect to units, however, as a tool for the qualitative analysis of resilience, this is seen as permissible. The results of this model have been broken down and summarised in table 5.1 for both case studies.

$$\Psi = \frac{10^{17}\,\Sigma\, n_j i_j}{[(CC+R)+10^{-8}\,CHP(H+E)]\,\left[10^{-2}\,CHP_i+10^{-3}\,CHP_p\right]} \qquad (5.1)$$

Table 5.1- Resilience Results of Case Study 1 and 2

	Case Study 1	Case Study 2
Indicators of Resilient Design, $\Sigma n_j v_j$	2.28×10^{-1}	1.17×10^{-1}
Capital cost, CC ($)	5.77×10^{8}	2.52×10^{7}
Annual Revenue, R ($/year)	7.30×10^{7}	2.37×10^{7}
Chemical Hazard Potential, CHP	1.31×10^{10}	4.10×10^{10}
Critical population, P_c	4.00×10^{0}	5.00×10^{0}
Wider population, P_w	5.50×10^{5}	6.28×10^{6}
Environmental impact rating, E	1.00×10^{2}	5.50×10^{1}
Potential Impact	7.22×10^{8}	2.63×10^{9}
Chemical Hazard Potential due to Ignition, CHP_i	8.79×10^{7}	1.80×10^{8}
Chemical Hazard Potential due to excess pressure, CHP_p (kJ/mol)	1.38×10^{8}	3.07×10^{8}
Vulnerability	2.26×10^{8}	4.87×10^{8}
Resilience, Ψ	1.40×10^{-1}	9.12×10^{-3}

6 Discussion

6.1 System Resilience

It is seen that case study 2 scored significantly lower for resilient design. This is attributed to a limited consideration of technical factors beyond that of the most basic design, and little to no consideration of administrative factors. With no thought to many indicators, a considerable number scored low. This displayed the importance of resilience considerations at the early design stages to ensure a system is created with resilience at its foundations. Additionally, despite case study 1 scoring higher for resilient design, many indicators still scored low despite the detailed HAZID and LOPA that had been completed. This shows that design basis hazard analysis does not extend well to give resilience. This is significant as displays that industry-standard hazard analysis is not sufficient to consider resilience and a specified analysis is required; stressing the importance of the presented model.

Case study 2 scores significantly higher for potential impact compared to case study 1 despite a lower potential for economic impact and similar critical population and environmental impact ratings. A factor contributing to this higher potential impact is the CHP which is notably larger than that of case study 1 due to a much higher volume of material of a similar hazard level present on-site. However, the factor most strongly influencing this high potential impact score is the extremely high population density in the Mumbai-Pune Industrial Area, giving a high wider population value. This places the site in an area with significant potential impact on human health as the population density here is over 300 times the global average and over 10 times that of case study 1. Finally, the vulnerability of case study 2 is around twice that of case study 1 for similar reasons as discussed for potential impact which gave a high CHP for case study 2. The resulting drastically larger potential impact and slightly larger vulnerability for case study 2 compared to case study 1 validates the model's sensitivity to each component of resilience.

The resulting resilience values of case study 1 and case study 2 show a stark difference of two orders of magnitude between them. This effectively displays the impact of the combination of factors contributing to system resilience and shows good model sensitivity to resilient design, potential impact, and vulnerability.

6.2 Improvements to System Resilience

The design of case study 2 is now adjusted to improve system resilience. This is done through 2 methods to compare impact. Design A has increased resilience via the improvement of resilient design where the top 3rd of indicators scoring the highest

cost-benefit ratings are improved to give a value of 1. It should be noted that in practice, small incremental improvements will be made to resilient design, over the group improvement of multiple indicators. This will start with indicators of the highest cost-benefit rating, and an iteration of resilience calculated after each improvement. This is completed with the aim of reaching a permissible level of resilience with the minimum investment required.

Design B is made more resilient by hypothetically moving the plant to the location of case study 1, Houston, Texas, significantly reducing the human health impact rating; a large contributor to the low resilience of case study 2. Resilience and its basic contributing factors for each design adjustment are shown in table 6.1.

Table 6.1- Case Study 2, Adjusted for Improved Resilience

	Design A	Design B
Resilient Design	5.83×10^{16}	1.17×10^{16}
Potential Impact	2.63×10^{9}	2.76×10^{8}
Vulnerability	4.87×10^{8}	4.87×10^{8}
Resilience	4.56×10^{-2}	8.69×10^{-2}

Design A displays a significant increase in resilience when improving resilient design via only a handful of indicators. These changes will of course have associated costs, but beyond this will have a relatively low impact on the wider system. However, when this is compared to design B it is seen that improvements to significant contributors to potential impact and/or vulnerability can give a much higher contribution to resilience. Making adjustments via this strategy, however, can involve dramatic changes to a system design. Design B required a new plant location to be sought, an act that would cause serious disruption to the planning and implementation of this system. Changes to other factors of potential impact and/or vulnerability would incur similar levels of disruption. For example, to decrease the CHP, the strategy via which processes are completed must be significantly altered or the chemistry changed altogether. Therefore, in practice, the pathway to achieving improved resilience must be carefully considered.

6.3 Putting This Model to Use

Important work that must be completed to transform this model into a fully developed tool for resilience analysis is the development of a resilience database to comprehend the model results in an industrial context. By applying the model to a wide variety of process systems a resilience scale can be developed which should be evaluated to determine the resilience values associated with a permissible process design. Furthermore, it is suggested that a traffic light system should be developed, defining unacceptable, permissible, and exceptional resilience levels. This will provide clear and data-supported meaning to the results of the model, creating a useful tool for industrial application.

7 Conclusion

With process industry disasters continuing to occur the requirement to prepare for BDBEs, pushing hazard analysis beyond that of traditional approaches, is being recognised and the importance of resilience and inherently safe design is being appreciated. Despite this, a widespread understanding and accepted definition of resilience has not yet been developed. Additionally, existing resilience quantifying models aren't practical for industrial use as are arduous and require extensive system modelling to complete. Hence, the consideration of resilience across industry has been seriously limited.

This paper offers proposals for the clear identification and breakdown of resilience and the system characteristics contributing to it. This has supported the development of a model for the assessment and scaling of system resilience, created through its novel consideration via 3 key attributes: 1) resilience of design, 2) potential for severe impacts of BDBEs (considering economic, human health and environmental consequences), 3) vulnerability to BDBEs. The developed model offers an industrially relevant tool for use from the early design stage which also allows for the clear identification and comparison of pathways to resilience improvements, with investments guided by a cost-benefit analysis.

This model is intended for wide application throughout the process industry and should not require an in-depth understanding of a system or of process safety to complete. This is to offer a methodology that can be carried out by the competencies available to a project, giving a strategy for the accessible and widespread comprehension of resilience. With further data collection to provide industrial context to calculated resilience values, this presents a tool for the standardized measurement of resilience across process sectors. This proposal can sit alongside and integrate with established process safety methodologies (such as HAZOP, QRA, and LOPA) and has the power to transform resilience from an ambiguous concept into a simple and widely used design strategy, vital for its practical application throughout the process industry.

References

Azadeh, A., Salehi, V., Arvan, M. and Dolatkhah, M., 2014. Assessment of resilience engineering factors in high-risk environments by fuzzy cognitive maps: A petrochemical plant. *Safety Science*, [online] 68, pp.99-107. Available at: <https://www.sciencedirect.com/science/article/pii/S092575351400071X> [Accessed 13 February 2022].

Bruneau, M. and Reinhorn, A., 2007. Exploring the Concept of Seismic Resilience for Acute Care Facilities. *Earthquake Spectra*, [online] 23(1), pp.41-62. Available at: <https://journals.sagepub.com/doi/10.1193/1.2431396> [Accessed 17 December 2021].

Crowl, D. and Louvar, J., n.d. Chemical process safety. 3rd ed. New Jersey, USA: Prentice Hall, pp.245-316.

Darbra, R., Palacios, A. and Casal, J., 2010. Domino effect in chemical accidents: Main features and accident sequences. *Journal of Hazardous Materials*, [online] 183(1-3), pp.565-573. Available at: <https://www.sciencedirect.com/science/article/pii/S0304389410009465?via%3Dihub> [Accessed 7 February 2022].

Dimitriadis, V. and Pistikopoulos, E., 1995. Flexibility Analysis of Dynamic Systems. *Industrial & Engineering Chemistry Research*, [online] 34(12), pp.4451-4462. Available at: <https://pubs.acs.org/doi/pdf/10.1021/ie00039a036?casa_token=AM2lOEO7_h8AAAAA:W1RNVd4wtYkKkxRHim4kqGSLy3AfU-19RLYuqSzo8T_u_-5rSDYLGFWx0wWjIOSxsXtKO18nGlUAvPU_2A> [Accessed 9 February 2022].

Dinh, L., Pasman, H., Gao, X. and Mannan, M., 2012. Resilience engineering of industrial processes: Principles and contributing factors. *Journal of Loss Prevention in the Process Industries*, [online] 25(2), pp.233-241. Available at: <https://www.sciencedirect.com/science/article/pii/S0950423011001525> [Accessed 30 January 2022].

El-Halwagi, M., Sengupta, D., Pistikopoulos, E., Sammons, J., Eljack, F. and Kazi, M., 2020. Disaster-Resilient Design of Manufacturing Facilities Through Process Integration: Principal Strategies, Perspectives, and Research Challenges. *Frontiers in Sustainability*, [online] 1. Available at: <https://www.frontiersin.org/articles/10.3389/frsus.2020.595961/full#B31> [Accessed 5 November 2021].

Francis, R. and Bekera, B., 2014. A metric and frameworks for resilience analysis of engineered and infrastructure systems. *Reliability Engineering & System Safety*, [online] 121, pp.90-103. Available at: <https://www.sciencedirect.com/science/article/pii/S0951832013002147> [Accessed 4 January 2022].

Ghoroi, C., Shah, J., Thakar, D. and Baheti, S., 2021. Process Design and Economics of Production of p-Aminophenol. [online] Available at: <https://www.researchgate.net/publication/355806733_Process_Design_and_Economics_of_Production_of_p-Aminophenol> [Accessed 26 March 2022].

Gilbert, S., 2010. Disaster Resilience: A Guide to the Literature. *U.S. Department of Commerce National Institute of Standards and Technology*, [online] 1117, pp.1-113. Available at: <https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906887> [Accessed 10 January 2022].

Hewitt, G. and Collier, J., 2018. *Introduction to Nuclear Power*. Boca Raton: Chapman and Hall/CRC.

IAEA, UNEP, UNIDO, WHO, 2022. *Manual for the classification and prioritization of risks due to major accidents in process and related industries*. [online] Austria: International Atomic Energy Agency, pp.9-67. Available at: <https://www-pub.iaea.org/MTCD/publications/PDF/te_727r1_web.pdf> [Accessed 12 February 2022].

Jain, P., Mentzer, R. and Mannan, M., 2018. Resilience metrics for improved process-risk decision making: Survey, analysis and application. *Safety Science*, [online] 108, pp.13-28. Available at: <https://www.sciencedirect.com/science/article/pii/S0925753517313802?casa_token=EXojAxTC43QAAAAA:_mw7sYlUvkZYaacMG1FJg7i60RFu2v3uwF6GZr64mK1RKZ432sp1bxF0dCqKZWyzIQT2yAU8ZGA > [Accessed 26 January 2022]

Keybiodiversityareas.org. 2022. *KeyBiodiversityAreas.org*. [online] Available at: <https://www.keybiodiversityareas.org/> [Accessed 16 March 2022].

MacAskill, K., 2021. *Resilience Engineered - Demystify resilience with this three-part film series*. [online] The Resilience Shift. Available at: <https://www.resilienceshift.org/resilience-engineered/> [Accessed 11 November 2021].

Nuclear Decommissioning Authority, 2011. *NDA Prioritisation – Calculation Of Safety And Environmental Detriment Scores*. NDA, pp.1-19.

Orosz, Á., Pimentel, J. and Friedler, F., 2020. General Formulation for the Resilience of Processing Systems. *Chemical engineering transactions*, [online] 81, pp.859-864. Available at: <https://www.aidic.it/cet/20/81/144.pdf> [Accessed 9 January 2022].

Pitblado, R., Fisher, M. and Nelson, B., 2016. Dynamic Barrier Management – Managing Safety Barrier Degradation. *HAZARDS 26*, [online] (161), pp.1-8. Available at: <https://www.icheme.org/media/11811/hazards-26-poster-06-dynamic-barrier-management-a-novel-approach-to-a-critical-safety-problem.pdf> [Accessed 14 November 2021].

Scattergood, M., Haider, M., Alenezi, M., Hoarle, J., Vesey, F. and Youssef, B., 2020. *Process Design and Economics of Production of Ammonia and Urea*. Undergraduate. University of Sheffield.

Taleb-Berrouane, M. and Khan, F., 2019. Dynamic Resilience Modelling of Process Systems. *Chemical engineering transactions*, [online] 77, pp.313-318. Available at: <https://www.aidic.it/cet/19/77/053.pdf> [Accessed 8 November 2021].

Yodo, N. and Wang, P., 2016. Engineering Resilience Quantification and System Design Implications: A Literature Survey. *Journal of Mechanical Design*, [online] 138(11), pp.1-13. Available at: <http://asmedigitalcollection.asme.org/mechanicaldesign/article-pdf/138/11/111408/6400827/md_138_11_111408.pdf> [Accessed 12 December 2021].