Quantifying Ease of Control for Inherently Safer Process Design and Optimization

Denis Su-Feher[1,2], Yogesh Koirala[1,2], Efstratios Pistikopoulos[2], & M. Sam Mannan[1,2]

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

Current inherently safer design strategies in the conceptual design stage focus on reducing the overall hazard of a process plant without considering the operability of the process. The process is first designed to be inherently safer with respect to a nominal, steady-state case. Then, after the process is designed, layers of protection are added and operability issues are addressed. However, this sequential design approach does not account for the impact of the design itself on the operability of the facility. A particular design may be safe with respect to its steady-state operation, but may suffer from operability issues. For example, an intensified process may contain less of a hazardous substance and thus be inherently less hazardous, but the design may restrict the controllability of the process, thus making the design have a higher risk and be more prone to loss. A considerable depth of research has been done to simultaneously optimize the design and control system of process plants, but no such approach has integrated inherent safety, only seeking to produce an economically optimal design rather than a safer one.

The objective of this research is to implement a strategy to simultaneously design and control an inherently safer plant. The Parametric Optimization and Control (PAROC) framework will be used as a basis to simultaneously design the plant and the controller. Different inherently safer design indices will be integrated into PAROC, and the operability, safety, and economic profitability of the results will be compared.

An extensive literature review identified metrics by which controllability of a process plant can be identified and optimized along with the design, as well as inherently safer design indices that can be implemented into the PAROC framework. These metrics and inherently safer design indices will be compared to create a new index for the integration of inherently safer design and control.

With process systems and their dynamics becoming increasingly complex, consideration of operability issues in the design stage becomes even more necessary to prevent incidents. The integration of inherently safer design and control will substantially reduce operability issues that result from an uncontrollable process design and allow for greater tolerance and ease of control.

Keywords: Inherent Safety, Multi-parametric programming, Design, Control

Introduction

The goal of chemical process plant design is to create a process that is both profitable and safe. An unprofitable plant will not sustain its operation, and an unsafe plant will not be profitable because of the losses it will incur when an incident happens. As such, managing risk is a necessary part of process plant design, as it maintains costs so that the plant can be sustained, while maintaining safety levels to prevent costly incidents.

On December 3, 1984, at a Union Carbide facility in Bhopal, India, 25 tons of Methyl Isocyanate (MIC) spilled from a storage tank and formed a toxic vapour cloud, killing over 2000 civilians and injuring over 20,000 more. MIC was an intermediate used to create carbaryl from methylamine and phosgene. However, at the time there was another reaction pathway available that produced the same product from another, less hazardous intermediate (Crowl & Louvar, 2013). If the less hazardous pathway had been used instead of MIC, then the 1984 disaster at Bhopal could have been avoided entirely. Though failure of many of the added prevention and mitigation measures resulted in more deaths than would have been expected from such an incident, the lack of inherent safety was the reason there was any incident at all.

The traditional approach to managing risk in the chemical process industry has often been to accept the existence of hazards in a process and to implement programs to manage the risk involved. However, in many cases such as that of Bhopal, this method has been proven to be costly and ineffective. Although opportunities for prevention and mitigation appear in the middle of the design process, the number of available inherent safety options decreases as the design proceeds, as shown in Figure 1 (Hurme & Rahman, 2005). Adding preventive and mitigative barrier later are often costly and not as effective as reducing the risk inherently, meaning that if inherently safer design practices are not considered in the earlier stages of design, then costlier and/or less effective prevention and mitigation methods will have to be used instead. However, in order to implement inherently safer design, the safety of different designs must be measured. Methods such as Hazard and Operability Studies (HAZOP), Fault Tree Analysis (FTA), and Failure Mode Effect Analysis (FMEA) can be used to address different aspects of risk assessment, but all of them require detailed information that may not be available in early stages of plant design. Quantitative inherently safer design indices, on the other hand, require relatively little information and can be used to assist risk-based decision-making in the early stages of plant design.

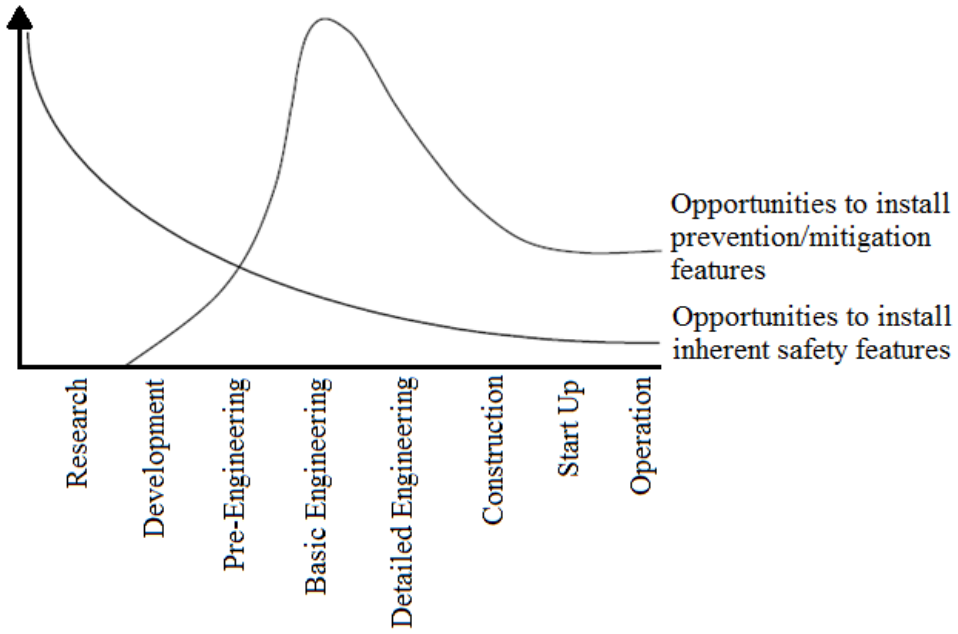

Figure 1. Opportunities for safety in various stages of plant design (Hurme & Rahman, 2005).

Inherently Safer Design Indices

Inherently safer design (ISD) is a philosophy for addressing safety issues that focuses on reducing the risk involved with hazardous operations by simply removing or reducing the hazards. Some principles, or guidewords, of inherently safer design are shown in Table 1 (Kletz, 1998).

Table 1 (Kletz, 1998). Inherent Safety Principles and Definitions

Inherent Safety Principle	Definition
Intensification	Using smaller quantities of hazardous substances
Substitution	Using less hazardous materials in the process
Attenuation	Using less hazardous conditions, or using the same material in a less hazardous form
Simplification	Reducing complexity in operational design to make operational errors less likely
Limitation of Effects	Reducing the severity of consequences associated with process design
Error Tolerance	Making the process resilient to disturbances
Ease of Control	Reducing the amount and complexity of control necessary to operate the process

These guidewords represent different ways to make a process design inherently safer by entirely eliminating aspects of the process that introduce hazard, and therefore risk. However, in the act of eliminating one of these guidewords, it is possible to introduce more of the others, and thus make the process less safe (Kirwan, 2009). Therefore, it is vital to create a comprehensive index that quantifies all of these principles, so that the total inherent safety can be measured.

The need for better risk assessment methods for the safer design of chemical processes has driven a substantial amount of research for more comprehensive ISD indices. Ever since Trevor Kletz popularized ISD in his 1978 article entitled, “What you don’t have can’t leak,” there have been numerous indices published that attempt to quantify different principles of inherent safety (Kletz, 1978). Table 2 indicates summary of some of these indices and their contributions.

Table 2. Inherently Safer Design Indices and their Contributions

Inherently Safer Design Indices	Contributions
Dow F&EI (AIChE, 2016)	First safety index reported in literature, and most commonly used in industry. Evaluates material properties and process conditions.
Dow CEI (AIChE, 1994)	Evaluates toxic effects and distance to neighbouring plants and communities to assess acute health hazard potential to them.
Mond Index (Tyler, et al., 1979)	Extends Dow F&EI by evaluating toxicity of chemicals.
INSET Toolkit (Mansfield, 1997)	Provides a guide to creating an inherent health and safety index.
HIRA (Khan & Abbasi, 1998)	Integrated material factor with operating conditions based on thermodynamic properties and expert opinions to find a damage radius under given overall conditions.
ISI (Heikkila, 1999)	First inherent safety index reported in literature. Quantifies minimization, moderation, substitution and simplification in terms of a ranking.
I2SI (Khan & Amyotte, 2004)	Extends ISI by weighing thermodynamic data and expert opinions to determine a risk ranking in terms of damage radius.
PSI (Shariff, et al., 2012)	Quantifies inherent safety of process streams during simulation work in the preliminary design stage that influences explosions.
RISI (Samith Rathnayaka, 2014)	Extends I2SI by evaluating frequency as well as consequence to obtain a risk ranking.

Although a substantial amount of work has been put into quantifying inherent safety, most of the current literature has focused on identifying the effects of intensification, substitution, attenuation, and simplification. Ease of control has not yet been fully quantified as an inherent safety principle.

Ease of control is the idea that, although "what you don't have can't leak," what you have left can still hurt you if it can't be controlled. A process with a larger amount of hazardous material may still be preferable to a process with a smaller amount of hazardous material if the process with a smaller amount of hazardous material requires a larger, more complex control system. A larger, more complex control system may be more likely to fail, and can be more prone to both mechanical and human error than a simple control system (Leveson, 2011). This increases the frequency of failure of the control system, which can have catastrophic effects. Since risk is a function of both consequence and frequency, it is important to consider some measure of frequency of failure in the early design stages.

Ease of control can be visualized in the form of a Swiss cheese model, as shown in Figure 2 (Reason, 2000). In the Swiss cheese model, loss occurs when accident trajectories manage to pass through multiple layers of protection. The layers of protection in this example are the process design and the process control system. The area covered by holes in each layer represents the frequency of failure of that layer. The frequency of failure of the entire system, then, can be approximated as the product of the total area of the holes in each layer, assuming that each layer is independent.

Quantifying ease of control, therefore, allows for the quantification of the total frequency of failure for the entire system. If the process design is optimized without considering ease of control, then there could be more holes in the process control system, meaning that any holes in the design itself will increase the risk of the total system. However, if the ease of control is considered, then it is possible that many of the holes in the process control layer can be eliminated with only a slight change to the process design protection layer.

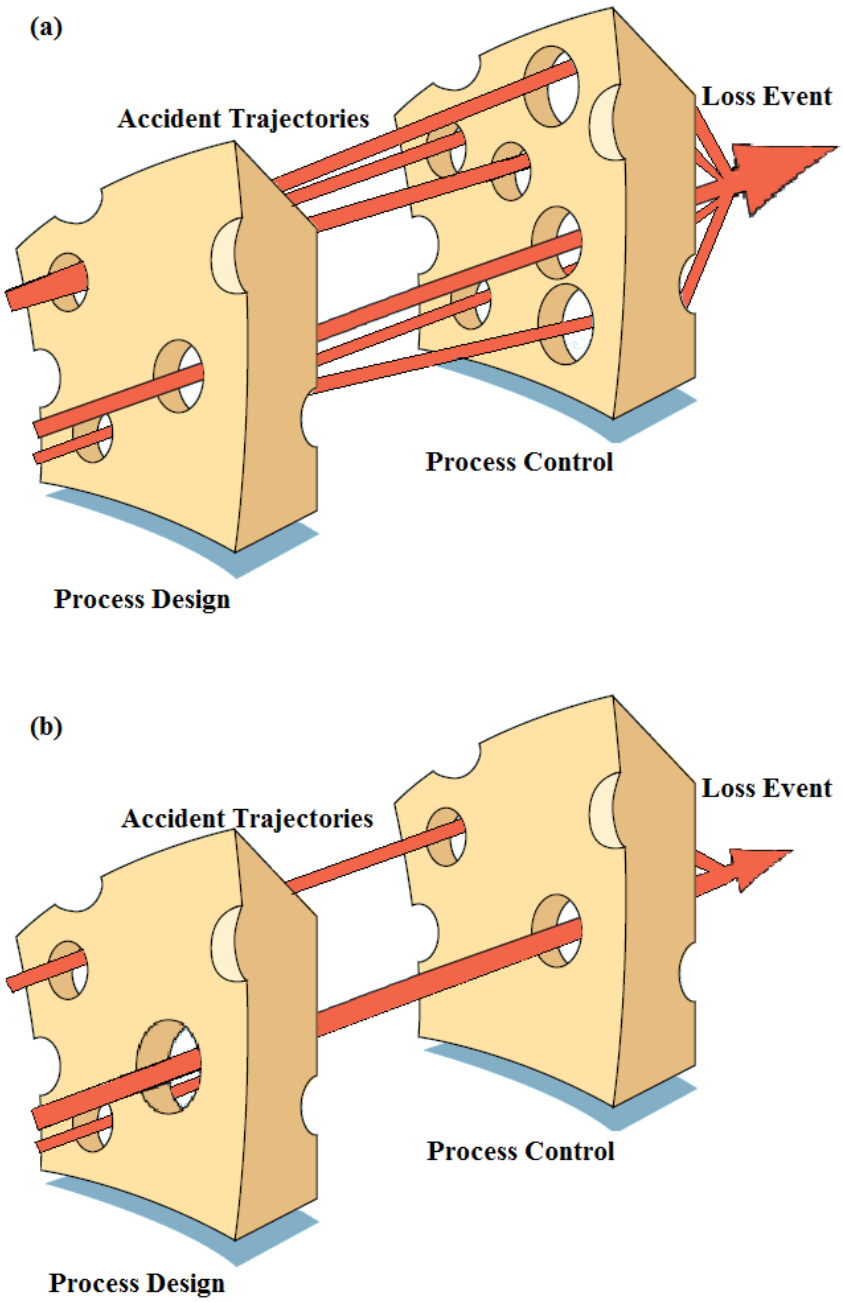

Figure 2. Process design and controls optimized for (a) design only, or (b) design and ease of control (Reason, 2000).

The aim of the present work is to define a process to quantify ease of control in order to create inherently safer processes. Several controllability indices are introduced as factors that can quantify ease of control. The vinyl acetate monomer production process is introduced as a possible case study to validate these indices for the control of exothermal packed bed reactors. The Parametric Optimization and Control (PAROC) Framework is introduced as a tool to design and control this reactor system. An equation for the quantification of controllability is proposed as an overall ease of control index, and this ease of control index is proposed to be implemented in a larger safety index.

Development of a Process for Quantifying Ease of Control for Inherently Safer Design

Definition

The process for quantifying ease of control for inherently safer design is shown in Figure 3.

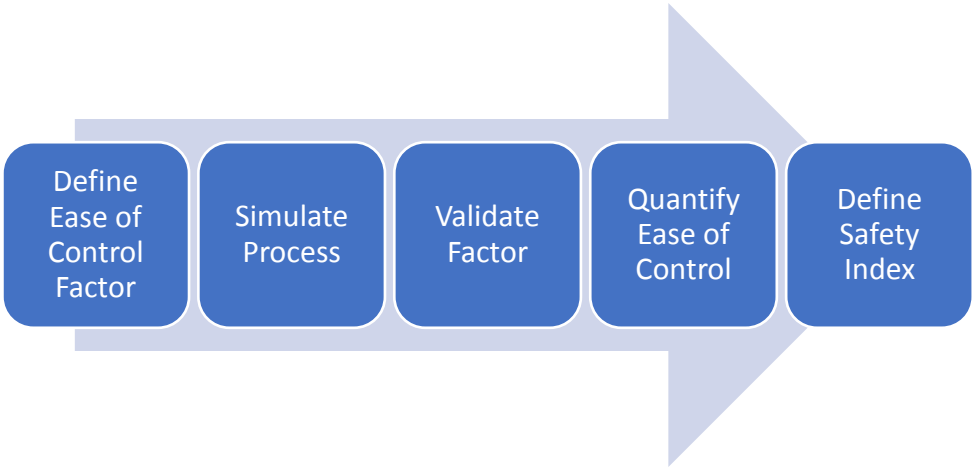

Figure 3. Proposed steps for quantifying ease of control.

The framework for quantifying ease of control for inherently safer design starts with defining a factor or group of factors that may influence ease of control.

This factor must:

- Be recognizable and quantifiable
- Indicate and benchmark future control performance
- Be able to measure the complexity and quantity of control needed to some degree

A number of representative processes must be simulated and controlled to optimality. These processes may be the same for each ease of control factor.

These processes must:

- Be representative of a specific type of process of interest (Examples: LNG dehydration, batch exothermic polymerization)
- Contain a variety of control schemes with different levels of complexity, and variables to be controlled

Each ease of control factor must be validated for its predictive power.

Validation questions asked may include:

- To what extent does the factor predict the complexity of the control system?
- To what extend does the factor predict the stability of the optimal control structure (eg. error and noise reduction)?
- To what extent does the factor predict the timeliness of the response?

Each ease of control factor must then be combined together into a single ease of control index.

Each factor must be:

- Scaled according to the uncertainty of its effect on the control system
- Weighted according to its prediction power and the importance of the effects it predicts

Finally, the total ease of control index must be brought into the context of a larger safety index.

Possible forms of this may include:

- Dividing the risk value estimate of the inherent safety index by the ease of control
- Factoring ease of control into the probability term of the risk estimate
- Adding safety credit factors to the final risk for improving ease of control

Case Study: Controllability in Vinyl Acetate Monomer Plant Design

A qualitative case study is presented to give a clearer understanding of how to apply the process for defining ease of control for inherently safer design.

Defining Ease of Control Factor: Controllability

The ease of control of a process is heavily dependent on the process's controllability. Controllability is an inherent property of a process that measures the ability and ease at which a process can achieve and maintain a desired equilibrium value despite disturbances and uncertainties. It has been shown that the design of a process can have a huge effect on its controllability and thus on its safety (Ziegler & Nichols, 1943). For example, certain process designs can have regions of instability that an inherently more controllable design may not have. If there is a region of instability near a steady-state, then attempting to control the system at that steady-state might be impossible, and another, less economically feasible steady-state would have to be used instead (Aris & Undson, 1958). These unstable regions would have to be addressed through either more control action, or less optimal set points, making the process system more complex, costlier, and potentially less reliable as a whole. A number of methods have been developed to measure different aspects of the controllability of both linear and nonlinear processes. They are displayed in Table 3. All of these methods take into account dynamic aspects of the process.

Table 3. Controllability Indices

Controllability Index	Summary	Linearity
RGA & BRGA (Bristol, 1966) (Kariwala, et al., 2003)	RGA defines a matrix that measures the effect of manipulated variables on controlled variables. BRGA extends it to block decentralized control.	Linear
NBRGA (Manousiouthakis & Nikolaou, 1989)	Extends BRGA to nonlinear systems.	Nonlinear
IMC (Garcia & Morari, 1982)	Creates an upper bound of controllability by assuming that the ideal controller is the inverse of the chemical process transfer function.	Linear
RHTP zeros (Holt & Morari, 1985)	RHTP zeros define areas where instabilities in control response may occur. The only way to move a RHTP zero is to change the process design. A controllable process must remove as many RHTP zeros as possible.	Linear
Input-Output Controllability (Zafiriou, 1994)	Defines eight rules for a controllable process.	Linear
Nonlinear Zero Dynamics (Trickett, 1994)	Quantifies the effect of the inverse responses in nonlinear systems for limited types of systems.	Nonlinear
Relative Order (Daoutidis & Kravaris, 1992)	Defines the pole excess of the transfer function. Quantifies how inputs directly affect outputs.	Nonlinear

For nonlinear systems, it has been shown that controllability analysis based on a linearized form of the system in many cases provides correct information, even if the system is strongly nonlinear (Morari, 1992). However, it has also been shown that this is true at steady-state, but not at wide operating regions, such as start-up, shutdown, and batch or semi-batch processes, and is not satisfactory for processes that have high degree of nonlinearity. Thus, for nonlinear processes, the accuracy of different control methods will have to be validated for different processes.

Simulating the Process: Vinyl Acetate Monomer Production

The vinyl acetate monomer plant was chosen for the purposes of defining controllability's effect on ease of control, as shown in Figure 4.

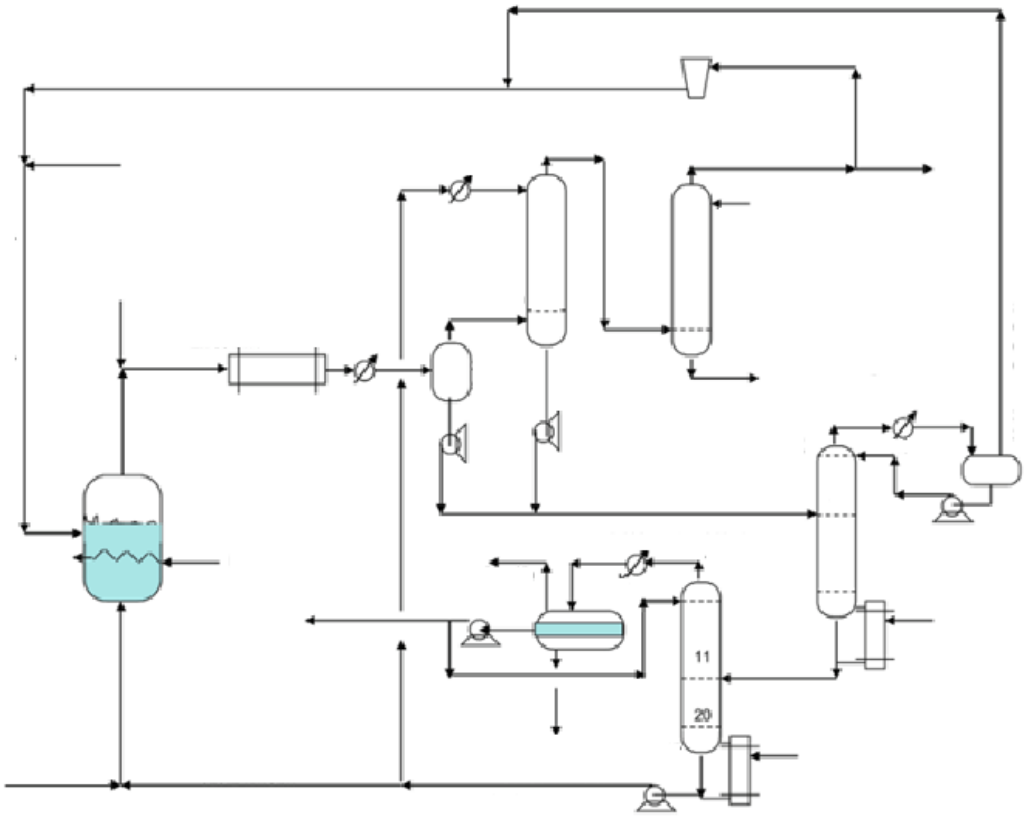

Figure 4. Vinyl Acetate Monomer Plant (Luyben, 2011)

Matlab can be used to simulate a reduced version of the vinyl acetate monomer production process system. As there are a number of important variables to control, as well as a number of variables that can be manipulated to control them, this process represents a case study of similar exothermic reaction packed bed reactor systems. Other, similar exothermic reaction packed bed reactor systems should be studied as well to determine the range of systems that the controllability index can be generalized to.

Validating Ease of Control Factor: PAROC

The Parametric Optimization and Control (PAROC) framework is a tool that provides the means for the simultaneous design and control of process systems (Pistikopoulos & Diangelakis, 2015). It starts with a high-fidelity model analysis of the chemical process, in which ODE's and PDE's are implemented into optimization software, following a first principle based approach to capture the entirety of the process. However, because solving such a complex system usually requires too much computation time to be economically feasible, model reduction techniques are used to linearize the high-fidelity model. Next, the control system is implemented using multiparametric receding horizon policies. Finally, the difference between these policies and the original high-fidelity model are used to validate the process. With exception of the model reduction of the design and multi-parametric programming to determine the control structure, both of which only need to be performed once, the process is iterated until the error is minimized.

PAROC allows for rapid, repeatable simulation of realistic control structures and the creation of optimal process designs under various conditions. PAROC has been implemented in the gPROMS software, and can be used to solve the simultaneous design and control problem to obtain the optimal process design and controller.

Quantify Ease of Control Factor

An equation can be proposed to find the total ease of control as a function of the proposed factors. An example is given in (1).

$$E = \prod_{i=1}^{n} w_i F_i \tag{1}$$

Define Safety Index

The ease of control factor can be added to any inherent safety index according to (2). Possible inherent safety indices are listed in Table 2.

$$R = \frac{\mathrm{ISI}}{E} \tag{2}$$

Conclusions

The background and process for quantifying ease of control for inherently safer design are discussed in this paper. A process with a larger amount of hazardous material may still be preferable to a process with a smaller amount of hazardous material if the process with a smaller amount of hazardous material requires a larger, more complex control system, as a large control system is more prone to failure. A process for quantifying ease of control is discussed, and a case study demonstrating how this process can be applied is explored.

Nomenclature

Symbol	Physical Meaning
E	Ease of control index
w	Weight for ease of control factor
F	Ease of control factor
ISI	Inherent safety index value

References

AIChE, 1994. *Dow's Chemical Exposure Index Hazard Classification Guide.* 1st ed. New York: American Institute of Chemical Engineers (AIChE).

AIChE, 2016. *Dow's Fire and Explosion Index Hazard Classification Guide.* 7th ed. New York: American Institute of Chemical Engineers (AIChE).

Aris, R. and Undson, N. R., 1958. An analysis of chemical reactor stability and control-I The possibility of local control, with perfect or imperfect control mechanisms. *Chemical Engineering Science,* 7:121-131.

Bristol, E. H., 1966. On a new measure of interactions for multivariable process control. *IEEE Trans. Automat. Control,* AC-11:133-134.

Crowl, D. A. and Louvar, J. F., 2013. *Chemical Process Safety.* 3 ed. Noida: Pearson India Education Services Inc.

Daoutidis, P. and Kravaris, C., 1992. Structural Evaluation of Control Configurations for Multivariable Nonlinear Processes. *Chemical Engineering Science,* 47: 1091-1107.

Garcia, C. E. and Morari, M., 1982. Internal Model Control 1. A Unifying Review and Some New Results. *Ind. Eng. Chem. Process Des. Dev.,* 21: 308-323.

Heikkila, A.-M., 1999. *Inherent Safety in Process Plant Design, An Index-Based Approach,* Espoo: Helsinki University of Technology.

Holt, B. R. and Morari, M., 1985. Design of resilient processing plants—VI, The effect of deadtime on dynamic resilience. *Chemical Engineering Science,* 40: 1229-1237.

Hurme, M. and Rahman, M., 2005. Implementing inherent safety throughout the process lifecycle. *Journal of Loss Prevention,* 18: 238-244.

Kariwala, V., Forbes, J. F. and Meadows, E. S., 2003. Block Relative Gain: Properties and Pairing Rules. *Ind. Eng. Chem. Res. ,* 42: 4564-4574.

Khan, F. I. and Abbasi, S. A., 1998. Multivariate Hazard Identification and Ranking System. *Process Safety Progress,* 17: 157-170.

Khan, F. I. and Amyotte, P. R., 2004. Integrated Inherent Safety Index (I2SI): A Tool for Inherent Safety Evaluation. *Process Safety Process,* 23: 136-148.

Kirwan, B., 2009. Incident reduction and risk migration. *EUROCONTROL Experimental Centre,* 49: 11-20.

Kletz, T., 1978. What you don't have, can't leak. *Chemistry & Industry,* 9124: 289-292.

Kletz, T., 1998. *Process Plants: A handbook for inherently safer design.* Bristol, PA: Taylor & Francis.

Leveson, N., 2011. *Engineering a Safer World: Systems Thinking Applied to Safety.* Cambridge: The MIT Press.

Luyben, W. L., 2011. Design and Control of a Modified Vinyl Acetate Monomer Process. *Ind. Eng. Chem. Res.,* 50: 10136-10147.