Inherently Safer Design – Designing Inherently Safer Plants

Recommended reading: Trevor Kletz, Paul Amyotte: Process plants – A handbook for inherently safer design, CRC Press, 2010

Lesson outline – Edit Székely, PhD

Is there any existing safe plant? *

Everything we do have risks. Thus, we cannot talk about something being safe. We must be willing to take some level of risks, but this does not mean, that we should not assess the probability of hazards, when those could be eliminated. The method we should follow is coming from the same place as* the principles of Occupational Safety and Health, therefore we must eliminate any hazard if we can. If we cannot, then we must ensure collective protection; if that is not possible, then we can use personal protective equipment.

Following the thread is clear, that the more earlier we pay attention to the factors determining the future safety designing a plant, the safer a plant will be. A significant amount of risks cannot be eliminated, even after completing the detailed risk assessment (right before building the plant, or continuously on an operating plant), we are only able to moderate their impacts.

In case of chemical plants, it is important from the start, even before developing and finalizing the reaction path, that a team of individuals coming from diverse fields should evaluate the progress of the design (chemist, chemical engineer, safety technician, people with practical knowledge regarding to plants, etc.). This is essential for safety, furthermore *a significant amount of investment and operation cost is tied to the safety equipment installation, maintenance, and continuous testing, and reporting everything mentioned before. These costs could be cut, if there is no need for a specific equipment.

What are the determining factors of risks in a soon to be existing or in an already existing plant? (Without being exhaustive, here are a few examples)

- The nature of the used substances (physical, chemical, biological properties, for example reactivity, toxicity, consistency, flammability, etc.) and its quantity
- The applied operations (volume, temperature, pressure, endotherm/exotherm, single or multiple input-output control etc.)
- Storing and transporting methods, quantities stored and transported
- Errors caused by human activity, such as repairing*

What methods can we apply, and what should we think about*, and what can we do?

1. Intensification and minimalization

Despite increasing the efficiency of a reaction or a separation we can, for example, decrease reactor volume. But we should not only think about the producing processes, but about storing, too. Do we really need to store huge amount of dangerous waste or intermediate? Is it possible to reduce the storing needs with the optimization of material transporting/handling, or with an in-situ production of a reagent, or with synchronizing each step of the technology better? if applying better, more efficient technological steps (which could be more expensive separately*), can we reduce the number of operating units, and shortening the length of pipelines, transporting routes?

The cause of the catastrophe at Bhopal, which killed over 2000 people in 1984, was the leaking of an intermediate called methyl-isocyanate from a storage unit. Although for the catastrophe to occur, it
needed numerous separate causes (significant amount of water got to the storage unit believed to contain 40 tons of methyl-isocyanate. Because of the water, an exotherm reaction started, temperature started rising significantly, and the methyl-isocyanate mixed with steam got out into the airspace). It is clear, that the catastrophe could have been avoided, if the methyl-isocyanate had not been stored in huge amounts around the factory.

*How efficiency can be increased? – Examples*

a) If the conversion is low, we separate the remaining reagent and recirculate it (this could be economical), but it means more separation steps, increased stream and transport volume. All of them decreases the safety of the plant. Occasionally, because of the low conversion, the final size of the plant is 3-4 times the optimal. The causes of low conversion are:

- The mixing is not efficient enough. Whilst in laboratories, the efficient mixing can be solved, in industrial scale is often the not-efficient mixing is what worsens the whole operation’s efficiency. Formerly, nitroglycerin was synthetized in huge, chilled tanks with batch reaction using glycerin and nitric acid in the presence of sulfuric acid. The reaction is exotherm, and the overheated solution can lead to explosion, thus the temperature must be watched. The reaction is excessively fast, the circa two hours reaction time is caused by bad mixing. The redesigned equipment is a small, intensively mixed, continuous batch reactor with average duration of stay being two minutes, and it is followed by a separation supported by a centrifuge. The reagents are intensively mixed in the entry point in an injector. The new method contained more explosives in the pipelines, than in the reactor and the separators, they contained circa five kilograms at the same time.

- The inherently slow reaction. Conceivable, that the reaction is inherently slow (the reaction rate coefficient is small). The increased temperature and/or pressure can fasten the reaction. Often, the plant is already operating on the highest possible temperature, without producing significant amount of side-product, and the reaction rate is limited by the low concentration. The higher concentration can increase the reaction rate, but it could worsen the control over the reaction (for example exotherm reaction). Catalysts can be used to increase reaction rate. If any of those ideas do not give a solution, then we can use a pipe reactor, which can be safer, than a batch reactor with a similar volume. The batch reactor is less more likely to leak, then a pipe reactor, however when it leaks, huge volumes get out at the same time. The mixing in the pipe reactor is determined by the flow rate, and it can be improved with relatively cheap and low-maintenance static mixers. Alternative of the long pipe reactor could be the loop reactor.

The increasing of efficiency often (but not always) leads to increased danger, for example rising the temperature or pressure. We should not forget, that we use pressure times volume multiplication to specify the danger of a pressurized vessel. Often decreasing the required volume, leads to the less risks over all.

b) If the heat transfer is not efficient enough, the heat exchanger will always constantly have significant amount of matter in it. Often this amount of matter could be similar* or more when compared to optimized reactor or distillation unit. The reasons for bad heat exchanges are:

- Too small average temperature difference
- Not adequate heat transfer surface
• Small heat transfer coefficient

2. Substitution
The substitution, if it can be solved economically, the best solution for avoiding dangers. Disadvantage is, it must be done in the earliest phase of development.

3. Attenuation (or moderation)
The attenuation primarily decreasing a plant’s inherent risks of storing and transporting. It is about choosing the proper state of matter, temperature, pressure.

4. Limitation of effects
The limitation of effects is already self-evident. Keeping the clearance, and building it in the plants, when we design the real* shape of it. The collective protection is always preferable to personal protection.

5. Simplicity
The more convoluted a system, the bigger the chance of a failure originating from wrong maintenance and repairs. This chance significantly decreases, if all the units are as simple as possible. In this sense, the production units specialized on one product are safer than multifunctional ones. Often the equipment becoming more convoluted originates from the safety equipment added later.

6. Avoiding knock-on effects
Keeping the clearance, and building it in the plants, when we design the real shape of it.

7. Making incorrect assembly impossible
Significant part of errors occurring due to inattention during maintenance can be prevented with proper design. For example, the inlet’s and outlet’s joint* should be different, or the pipelines should not be too long to be assembled wrongly.

8. Making status clear
For example, rising valve stem, instrument being transparent even with a glance, ergonomic design.

9. Tolerance of misuse
For example, a pump could be used as a step-up without damaging it.

10. Ease of control
The control of reaction, separation, flow rate, temperature, etc. is always a determinative problem. Always advisable to intervene simplest way possible. The measured signal, tolerance interval, point of intervention, method of control etc. can be designed beforehand, but it always needs fine-tuning during set-up.

11. Computer control
The computer software must serve the user, and not the other way around. The software’s user-friendly design significantly decreases the errors and the time for learning the ins and outs of the software.
12. Instructions and other procedures

Instructions should not try to cover every conceivable condition that might arise, otherwise it will be so long and complex no one will read them. The instructions for helping the worker, not protecting the writer.*

13. Life-cycle friendliness

Designing a plant, we should not only care about the safety of conceivable operating conditions, but we should also pay attention to it while dismantling the plant. Today we can even buy whole manufacturing plants, and dismantlability is a market interest.

14. Passive safety

It is a general Occupational Safety and Health principle, that passive protective measures are favorable to active (smaller the chance of errors), and collective protection is always preferable to personal protection.