Journal of Integrated Security Science

SAFETY AND SECURITY: WHAT ARE THE PARALLELS, AND WHY RESEARCH IS NEEDED?

Hans J. Pasman*

Research Professor Mary Kay O'Connor Process Safety Center, Texas A&M University, College Station, United States

Received 1 April 2017
Accepted 1 June 2017

Safety and Security are highly related. Both the safe and secure states would be perfect if no risk would loom. However, this situation will be utopian. With respect to safety we know life is full of risks which may be large, yet acceptable if we enjoy the activity or the situation, but when subjected to it involuntarily we want risk to be negligible. With regard to security the objective is identical: we want the risk of security breach to be negligible. Risk assessment has the objective to try to determine the magnitude of risks to judge their acceptability. Now, a safety risk has two components: the consequence of an accidental event and the probability of the event occurring. The former depends on the intensity of the exposure (in terms of power, impulse, shock pressure, heat, toxic concentration, radiation), the duration of exposure and the vulnerability of exposed people, of exposed responsive structures or that of the environment, together determining the damage or loss. The latter, the probability, depends on many factors of technical, organizational or human nature. In safety, we also make the distinction between personal safety of the worker in the plant environment, who may be directly in contact with hazardous material but can make use of personal protective equipment, and process safety which considers upsets and mishaps of the process occurring often suddenly and involving spread of hazardous material over relatively large areas and threatening the public. In security, this distinction is obviously not relevant from the point of view of the perpetrator.

As mentioned, the concept of security is much related to that of safety, and certainly to process safety. This is clearly true regarding the intensity of a damaging agent and the vulnerability of the exposed people and objects, yet security differs fundamentally of the concept of safety. This is in the sense that where in safety nobody wants the damage to occur, in case of security there is a malevolent individual, group or people that wants the damage done. As the objective of plant owner and society, and thus of government is to keep also in this case the risk low, the aim to cause intentional damage and preferably to cause the loss in a single event as large as possible, places the field of security is a fully different perspective.

Both good safety level and good security level require predictive assessment of possible damage consequences given a scenario of the release of energy or hazardous substance in a certain situation and the possible occurrence of domino effects. The obvious reason for identifying scenarios and predicting potential damage is that it enables installing preventive measures and

* Corresponding author (Hans Pasman)
Email address: hjpasman@gmail.com

ISSN: 2468-4546

protective structures that would reduce damage in the unfortunate case a scenario would unfold. So, there are parallels again, since the properties of substances, the physical spreading mechanisms upon release from containment and the action on exposed people and objects, will be the same. One subtle difference is, though, that the latter will be indicated by a perpetrator as 'targets'. A further difference and rather elementary one is the way a release is initiated. In safety risk, it is a release by an unforeseen failure of equipment due to wear or a design flaw, or wrong use, negligence and operating error. In a deliberate attack on a well-functioning process plant, storage facility or transportation system, initiation mechanism will be totally different. The mechanism will depend too on the intention behind the attack. Will it be to destroy as much as possible in order to deny the use of the product or to threaten people around and cause fatalities, or is it to steal material for selling it or to cause damage in terroristic attack elsewhere?

So, even where parallelism in both safety and security is largest, in elaboration differences are quite large and what is important is that the way hazardous material can be released, determines also the way barriers shall be designed. In intentional attack one can go for brute force by use of high explosives brought inside the plant, dropped into it from a distance by, e.g., a drone, or a person with a device propelling a projectile from outside the fence. In contrast, one can also intrude into a plant area, e.g., being disguised as a plant worker, and purposely sabotage the process or means of storage and transportation. Possibilities will affect decisions about optimal nature of the barriers, their structure, and placement.

A special initiating agent that only marginally gets consideration in safety but is very important in security, is the cyber threat. Quite a few types of barriers are control loops that consist of a sensor, processor and actuator. Hacking a plant's control systems can be a threat exerted from a remote spot. Hacking may disturb or even destroy the control and halt the process. Although in general there will be some protection regarding lightning, also generating directed powerful electro-magnetic pulse will be a potential threat that can be brought to bear at some distance.

Anyhow, estimating the likelihood of an occurrence in safety and security will be totally different. In safety, over the years very slow progress has been made to at least estimating the range of event rates to be expected. Where in the past risk assessments on a 'frozen' static situation were already notoriously inaccurate with respect to probability, step by step the dynamic operational risk by human activity is being considered as well. In security, no estimate is possible. This is because historical data fortunately are very few, so no statistics can be derived. Of course, one can make a guess on the basis of what an attacker would think is attractive which plant equipment would be a preferable target. This whole matter is very relevant when, with a limited budget decisions have to be made on how to protect best. So, hazard identification and very thorough definition of possible scenarios which depend on process, plant and environment will be of utmost importance. Failing to see a possibility can be fatal, but completeness is almost impossible and reliance must also be sought in sufficient degrees of resilience, which is another chapter. On the other hand, as in war games and operational research, game theory can be applied to weigh chances of an attacker against those of a defender given the scenarios defined and the layers of protection realized. Optimization will be a good research aim.

Altogether, it will be clear that given the complexity of possible scenarios, to protect the general public and involved plant personnel against possible effects of hazardous materials, being released accidentally or intentionally, and to save costly process equipment from these effects, it is

worth to spend a strong research effort on a wide variety of aspects. We hope to welcome in this journal many contributions of researches on various topics that will build and expand relevant knowledge to the benefit of all.