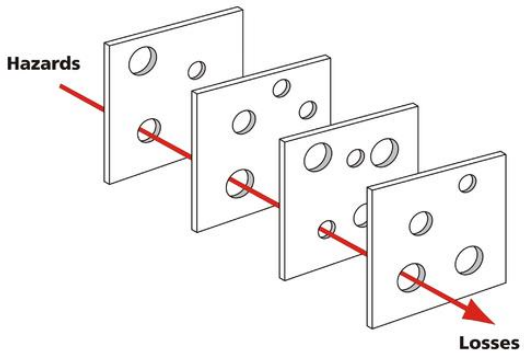
Process Safety Models: Cheese, Chains or Cords?

Harvey T. Dearden BSc CEng FIET FIMechE FInstMC FIChemE
SISSuite Ltd

The Swiss cheese model is often employed in representing process safety. The individual slices represent different defences or barriers, and the holes represent the potential for a barrier to fail. If the holes should align, all barriers will fail and the hazard consequence will be realised. Weaker barriers have bigger and/or more holes than stronger barriers. It usefully captures the idea of layers of protection, and of these being invoked in the order corresponding with the layer sequencing, but it relies upon the abstract notion of 'dynamic' holes that vary in size and location, and in illustration it requires a perspective drawing. It is an appealing illustration that immediately conveys the primary concern of multiple concurrent failures; it is perhaps less good at representing the integrated nature of process safety.



Swiss Cheese Model
(Source: Wikimedia Commons, Author David Mack)

Barriers or defences that consist of multiple elements are sometimes thought of as chains because the elements must all work together if the barrier is to be effective. This is not really an accurate analogy however. 'A chain is only as strong as its weakest link', because each link carries an identical load. This is not true of process safety protection 'chains'. In terms of protection, the 'strength' of a chain 'link-element' relates to the probability of its failing (or being failed) when needed. If the strength of a link is increased, (the probability of failure reduced) the strength of the entire chain is enhanced, since the strength of a protection chain corresponds with the aggregate probability of failure of all the link-elements. The 'all work together' concept is potentially useful for our purposes in modelling protection, but the 'weakest link' notion is so strongly associated with chains that this militates against their adoption.

As an alternative, we might adopt a model of a 'suspended load' which might be considered as more complete in representing the idea of an integrated system. In this model, (which can be illustrated without employing perspective), process safety is represented as an arch carrying a suspended load that represents process hazard. The arch represents inherent safety – those design provisions that mean there is low danger level even if the active systems should fail; a load-hazard above the arch cannot be realised as long as the inherent safety provisions are maintained. (But may be realised if uncontrolled changes are introduced that undermine the inherent safety provisions.) If the suspended load is dropped the hazard event will be realised. The load is suspended by a number of cords, each of which represents a different defence or barrier. These cables are of different lengths; the shortest will carry the load, but if it should fail the load will transfer to the next shortest. The cords may also have different 'strengths' corresponding with their probability of failure. A typical arrangement would

be a pressure control system backed up with a high pressure trip function, backed up in turn by a relief system. In normal operation the load is carried by the control system and the other cords are slack. It is only if the control system cord should fail that the load is placed upon the high pressure trip cord. If that cord should fail, or be disconnected by an override, the load will be placed upon the relief system cord. If all cords are compromised the load will be dropped and the hazard event will be realised.

A 'safety net' may represent conditional modifiers such as occupancy or probability of ignition etc.; this would only be invoked if the load was dropped, and models the possibility that the consequences might not be realised even if the hazard event should occur.

If a hazard is only present intermittently, so that an 'enabling condition' is required, this may be represented in the same manner, but with the load sat on a projecting support beneath the arch so that all the cords are slack; it is only when the support is removed that the hazard potential arises.

If a cord is too long, it will not provide any defence even if it is not itself compromised; it would be too late in restraining the load to supress the hazard. It would offer only the illusory appearance of a defence. This would be the case if a trip point was too close to the hazard for a trip to be timely (response time longer than the process safety time), or if an alarm was too late for effective intervention.

If protection provisions share some common elements, this may be represented by parallel cords suspended from a common cord (or vice-versa).

If a system such as 2 out of 3 voting is employed, this could be represented as three parallel cords each with a 50% load capacity, although this may be asking rather too much of a simple illustration.

No claim of complete fidelity is made and there is nothing so very profound here, but it is hoped the model will be useful in conveying an understanding of relevant concerns.

(To view an animated illustration of the model, visit www.sissuite.com)