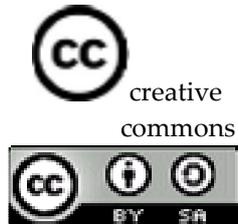Process Contracting Limited
20 Springs Park
Coylton
Ayr
Ayrshire
KA6 6QQ
tel 01292 571221
http://www.processforusability.co.uk
brian@processforusability.co.uk

Organizational Accidents:
From Swiss Cheese to Swiss Chateau

Brian Sherwood Jones
Process Contracting Limited
v1.0 22 March 2008

Summary

The Swiss Cheese Model of Organizational Accidents and the Swiss Chateau Model of Organizational Accident Prevention have been constructed and placed near Gruyere, Switzerland.

The models can be found via:
http://sketchup.google.com/3dwarehouse/search?uq=11342046068132504940

The Swiss Cheese Model has saved a great many lives, and advanced our understanding of accident causation considerably. As a consequence of this increased understanding, we are able to move on to a new model. The model proposed is the Swiss Chateau Model. This note summarises the need for the transition and outlines the Swiss Chateau Model.

Reason's Swiss Cheese Model of Organizational Accidents

The Swiss Cheese Model is shown below in Figures 1 and 2.

Figure 1- The Swiss Cheese Model, outside Gruyere.

Figure 2 – The Swiss Cheese Model, with the 'accident trajectory' from hazards to losses.

Jim Reason, in his book 'Managing the Risks of Organizational Accidents' (1997) introduced us to the Swiss Cheese Model, and the ideas of 'active failures' vs. 'latent conditions'. Introducing the world to the idea of latent conditions has done immense good. The idea has been generally assimilated, and we are ready to move to the next step in our understanding of how to prevent organizational accidents.

Misleading Affordances

The Swiss Cheese Model has a number of 'affordances' (Gibson) that may well have been unintentional, but which have set the scene for much thinking about organizational accidents. Reason points out that the defensive layers and their holes are in constant flux. This may get forgotten when looking at the diagram without such a reminder, but the following points stand even when it the flux is remembered.

Firstly, 'unsafe acts' only happen at the sharp end. What people do in the layers of defence is bring about latent failure conditions. The distinction between latent conditions and active failures is the delay in loss occurring, not the nature of the error, violation, or decision making. Regulators can commit violations under commercial pressure in just the same way as 'operators'. If we are to achieve further improvements in safety in the 21st Century, then this distinction needs to go. Reason pointed out that 'unsafe acts' should be seen more as consequences than as primary causes, but this has not really taken root. It may be that the comfort provided by the model has aided those who would rather not see active failures as consequences of latent conditions.

Next, the viewer is led to believe that 'the odd thing gets through' the layers of defence. This is a very comforting description; the reality is otherwise; we now recognize that complex system run broken. A regulatory failure, a management shortcoming, a design flaw goes straight to the sharp end. If the sharp end has the capacity to deal with that problem as well as do the day job, then there is no accident. The 'layered defence' is a mirage.

The concept of an 'accident trajectory' is puzzling epistemologically. Just what is it that can travel through a design flaw, a training shortfall and a procedural omission? There is no such single thing. There is no need for the holes in the cheese to line up; hazards come through each layer to operation.

The temporal sequence implied is not necessary or appropriate. The time lapse between a design or regulatory or management failure and an accident can be very long or very short, and no particular temporal sequence is required.

There is one series of defences lined up behind each other (definitely not in front of each other!). This comes from the concept of 'the organization' as a single entity. From the scene of the accident ('Losses' in Figs 1 and 2), the sharp end is plain to see, but maybe the blunt end looks homogeneous. In reality, it is anything but homogeneous; the blunt end comprises multiple stakeholders in a complex network.

Developments in our understanding since publication of the Swiss Cheese Model

Developments on two fronts have enabled us to progress from the Swiss Cheese Model. Developments in our understanding of how complex systems stay safe, and developments in the management of complex systems.

http://www.ctlab.org/ The work of Cook, Woods and others at CTLab provides a good summary of advances in our understanding of how complex systems stay safe. Their summary sheet:
http://www.ctlab.org/documents/BriefLookAtTheNewLookVerAA.doc.pdf
includes the Swiss Cheese Model, as is right. There are many aspects of our understanding now that are not easily accommodated within the model, however.

Our understanding of how to manage complex systems has improved considerably, and has been captured in International Standards, such as ISO/IEC 15288, ISO 13407, ISO TR 18529, ISO PAS 18152, ISO 9126. We can think about having a model of accident prevention based on the systems concepts in ISO/IEC 15288, rather than building a model that starts with the accident and works backwards. The 'concept of 'enabling systems' is powerful, not least because it allows issues such as clumsy automation to be placed in the correct system. The concept of process as an area of continuing concern, principally characterised by ownership and outcomes is a major step forward in our ability to manage the emergent properties of complex systems.

We can now start to use models of good practice in enabling systems and the system of interest as a fairly comprehensive, assessable, positive framework, rather than Generic Failure Types. We can emphasise the positive to eliminate the negative.

The Swiss Chateau Model of Organizational Accident Prevention

Gruyere has a very fine chateau, whose form inspired the construction of a virtual chateau as a model of the defences against organizational accidents. The original chateau is shown below in Figure 3.
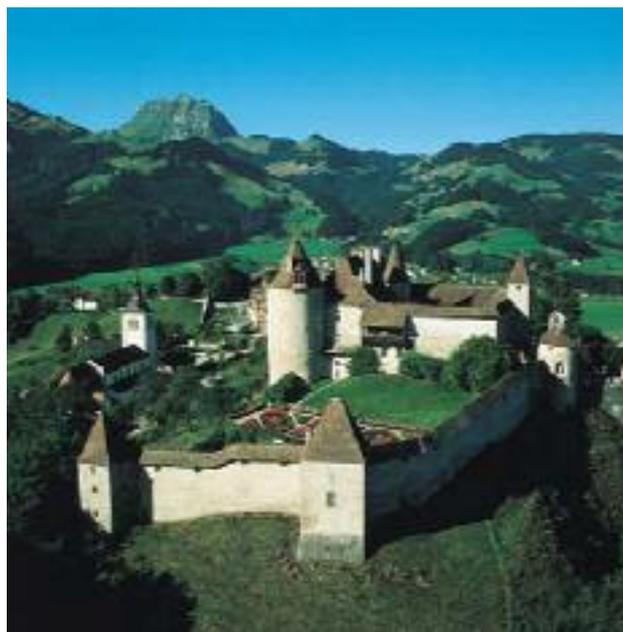

Figure 3 - Chateau Gruyere.

The Swiss Chateau Model, situated outside Gruyere, is shown below in Figure 4.
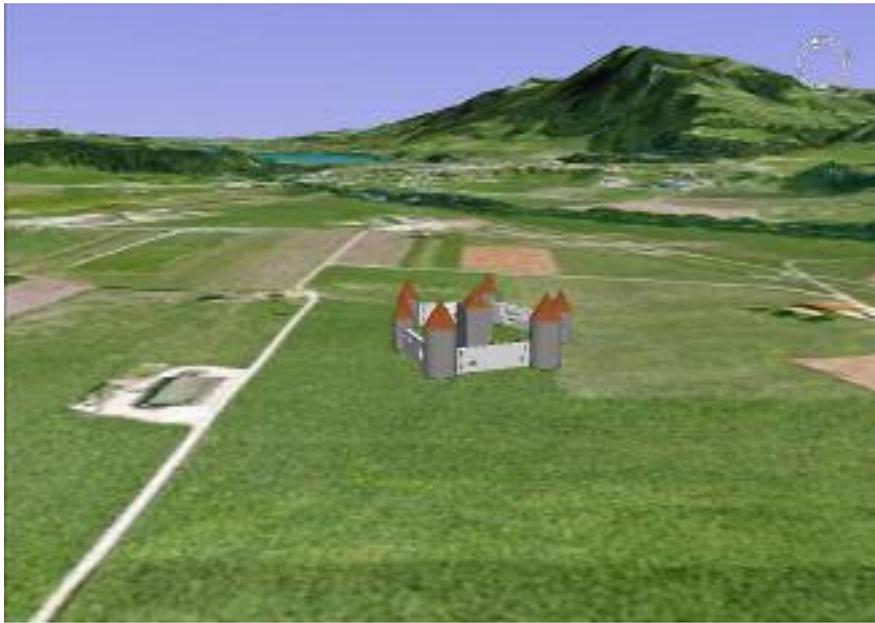

Figure 4 Swiss Chateau Model outside Gruyere.

The last line of defence in the centre of the model is the Crew; the people at the sharp end. This is 'the system of interest'. Defending them, at the first line of defence, are organizational 'enabling systems'. There are six of these, as shown in Figures 5, 6 and 7. All have large holes in their defences.
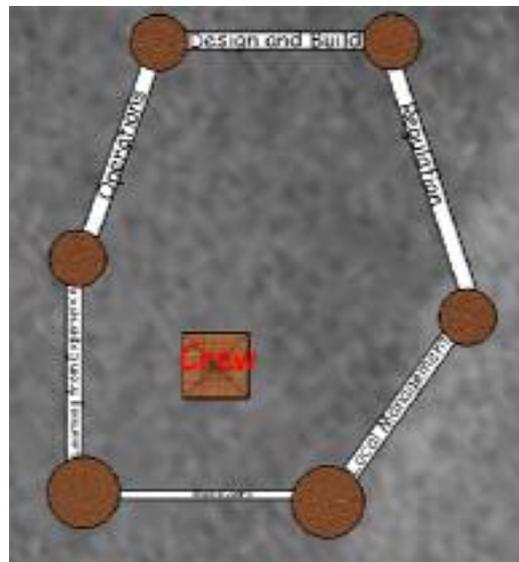

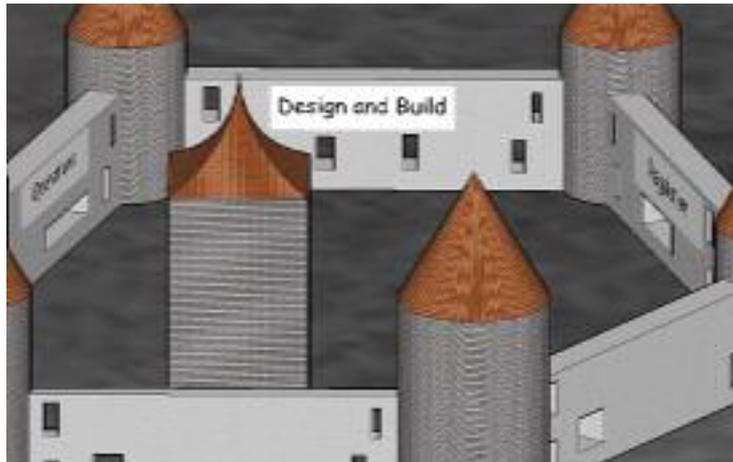Figure 5 - Swiss Chateau Model elements.

Figure 6 - Longer term enabling systems (Operations, Design and Build, Regulation).
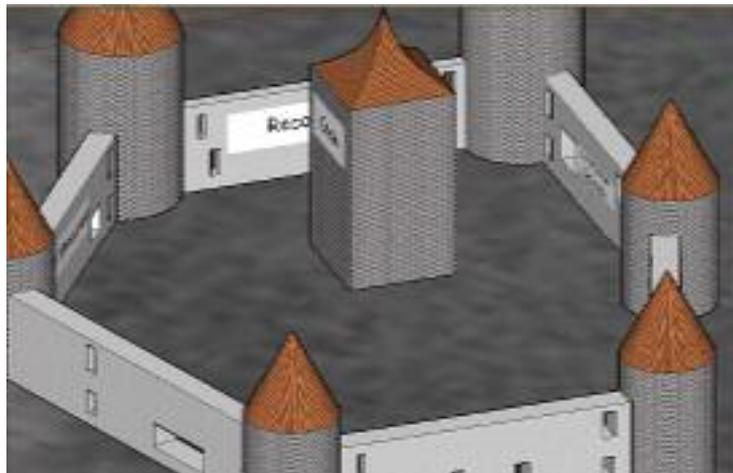

Figure 7 - Short term enabling systems (Local Management, Recovery, Learning From Experience).

The longer term enabling systems are as follows. Operations comprises the management of the enterprise that runs the system of interest e.g. a shipping company for a system of interest that is a ship. Design and Build embraces the supply chain for the system of interest e.g for an aircraft it might be Boeing and all its suppliers. Regulation comprises the regulatory system.

Nearer the crew in temporal terms and generally operating on shorter timescales are the following. Local management is the immediate management and supervision. Recovery includes both containment and recovery; an important aspect of a High Reliability Organization is the ability to bring in extra resources rapidly under circumstances of high demand. Learning From Experience is the system for learning from near-misses, surprise successes and incidents.

Purpose of model

The purpose of the model is to provide a framework for preventing organizational accidents (rather than having to explain them). The starting point is the role of management, rather than the evolution of an accident. Accidents inform the design of systems for safe management, but when designing such systems, it is better to start with the system than the accident.

Background to model

The background to the model is the type of systems thinking that went into ISO/IEC 15288, and which informed the work on Systemic Incident Analysis by the author and Vaughan Pomeroy.

Intentional affordances

Firstly, the model places the crew as the last line of defence, rather than the people nearest the accident. It also places people who see themselves as layers away from an accident in the front line.

It removes the idea of layered defences, and replaces it with the idea that the system runs 'broken' as a matter of course (see the work of Dave Woods and Richard Cook). Those hazards that get through the holes in the first line of defence cause the crew to perform 'integration work' (Lutzhoft). Putting people in the front line may have the benign consequence of increased urgency and focus.

Cheese is a pretty passive material. Replacing it with a more active defence metaphor gives some limited support to the idea of 'making safety'. It also conveys the move from a model about how accidents might happen, to a model about how they might be prevented.

The distinction between 'latent conditions' away from the accident and 'active failures' near the accident is removed (or even possibly reversed).

Locating the model in the same countryside as the Swiss Cheese model is intended to convey evolution rather than revolution.

Practical implications

The first implication is a change in approach; many new people are put in the front line, and the capability of each enabling system can be assessed against good practice before an incident. In practical terms, there are many fairly immediate implications for enabling systems; a self-assesment might be a good start.

Incident analysis is in a transitional stage; it knows that the sharp end is just the tip of an iceberg, but has not really taken a remit to go below the surface to the extent that would deliver real improvements in safety.

Lastly, it might make it clearer to people that the crew are the last line of defence, not the first.