# Human Error and Defense in Depth: From the "Clambake" to the "Swiss Cheese"

Justin Larouzée

# Human Error and Defense in Depth: From the "Clambake" to the "Swiss Cheese"

**Justin Larouzée**

**Abstract** After the Fukushima accident, a new concept of nuclear safety arouse: engineering thinking facing extreme situations. One of the specificity of emergency situations being a rise of social demand on engineering process, safety scientist have to make an anti-dualist move in order to improve collaboration between social scientists and engineers. In this aim, this article studies a case of efficient collaboration: the Swiss Cheese Model (SCM) of accidents. Since the early 1990s, SCM of the psychologist James Reason has established itself as a reference in the etiology, investigation or prevention of accidents. This model happened to be the product of the collaboration between the psychologist and a nuclear engineer (John Wreathall). This article comes back on the journey of the SCM and its fathers. It is based on an exhaustive literature review of Reason's work and interviews of Reason and Wreathall carried out in 2014. The study suggests that the success of the model is not so much due to appropriation of the work of the psychologist by the industrial community but to a complex process of co-production of knowledge and theories. To conclude, we try to highlight ways that should encourage, in the future, such collaborative ways of working.

**Keywords** Swiss cheese model · James Reason · John Wreathall · Coproduction · Collaboration

## 1 Introduction

The Fukushima nuclear accident that occurred in Japan, March 2011, and its aftermath reinforced the need of theoretic and pragmatic studies over industrial and social resilience. Since there is no end in sight to the accident, it also raised the issue of engineering thinking facing extreme situation [1]. Defined as "*engineering activities*

J. Larouzée (✉)
Centre for Research on Risks and Crises (CRC), MINES Paristech/PSL Research University, Sophia Antipolis, France
e-mail: Justin.larouzee@mines-paristech.fr



J. Ahn et al. (eds.), *Resilience: A New Paradigm of Nuclear Safety*,
DOI 10.1007/978-3-319-58768-4_22

*that are significantly impeded due to a lack of resources in the face of a societal emergency*", this new concept of nuclear safety insist on the link between engineering processes and social contingencies. In this paper we therefore try to shade a light on collaborative process where social scientist and engineers come to work together (more than side to side) in order to seek determinants of successful collaborations. The paper focuses on an historical case: the (so called) *Swiss Cheese Model* of accidents. Since the early 1990, the Swiss Cheese Model (SCM) of the psychologist James Reason has established itself as a reference model in the etiology, investigation or prevention of industrial accidents. Its success in many fields (transport, energy, medical) has made it the vector of a new paradigm of *Safety Science*: the organizational accident. A comprehensive literature review of Reason's work leads us to consider the SCM as the result of a complex (and poorly documented) collaboration process between the fields of research and industry; human sciences and engineering sciences. In a dualistic premise where research and industry would be two entities interacting but still separable, this collaboration would be understood as the appropriation of research work by the industrial world. However, the complexity of the genesis of the SCM forces an overcoming of this dualism to bring out a process of "co-production" of knowledge. As part of this research, the two main "fathers" of the SCM: James Reason (psychologist and theorist of human error) and John Wreathall (nuclear engineer) where interviewed by the author. These meetings shed a new light on a prolific era for the Safety Sciences field. We therefore hope to keep from a retrospective bias that tends to smooth and simplify facts. This chapter deals with the induced effects of the collaboration between a psychologist and an engineer in terms of models production. In the first section, we briefly present the two "fathers" of the SCM and the social and historical context in which their collaboration took place. In the second section, we focus on the effects of this collaboration over their intellectual and scientific productions. Note that prior knowledge of the SCM, its theoretical foundations and its main uses is requested (see, for example Larouzée et al. [2]).

## 2 The Fathers of the Model

This section presents the two fathers of the SCM. Reason a psychologist of human error and Wreathall a nuclear engineer. After presenting their backgrounds (Sects. 1 and 2), we present the social and industrial context in which they were brought to meet and work to create the first version of the SCM (Sect. 3).

### *2.1 James Reason, the Psychologist*

Reason gets a degree in psychology at Manchester University in 1962. He then works on aircraft cockpit ergonomics for the (UK) Royal Air Force and the US

Navy before defending a thesis on motion sickness at Leicester University in 1967. Until 1976, he works on sensory disorientation and motion sickness. In 1977 he becomes professor of psychology at Manchester University. In 1977, Reason makes a little action slip that will impact his scientific career. While preparing tea, he began to feed his cat (screaming with hunger). The psychologist confused the bowl and teapot. This was of great interest to him and he started a daily errors diary. That's how he started a ten years research on human error which resulted in a taxonomy (1987). After he became a referent on the issue, he was a keynote speaker in various international conferences on human error. During one of these conferences, he met John Wreathall, nuclear engineer, with who Reason built working relationship and "*strong intellectual communion*" (in his words). On their collaboration will be drawn the first version of the SCM. Since then, Reason kept working on human and organizational factors in many industrial fields.

## 2.2 John Wreathall, the Engineer

John Wreathall studies nuclear engineering at London University, undergraduate in 1969; he gets a masters' degree in systems engineering in 1971. Later he studies an Open University course "Systems Thinking, Systems Practice" based on Checkland's models of systems. This option brings the young engineer to human factors and systems thinking. From 1972 to 1974 he works on the British nuclear submarine design which allows him to access confidential reports on HRA by Swain. From 1976 to 1981, Wreathall works for the CEGB (English energy company), first as design reviewer for control systems then as an engineer on human factors in nuclear safety. As an acknowledged expert he was brought to participate in conferences organized by NATO and the World Bank called *Human Error* (book "*Human Error*" by Senders and Moray is the only published product from the 1981 conference of the same name). After meeting Reason there, they both started professional collaborations on accident prevention models (including SCM). His interest in the human factor brought him to several leading functions where he worked on human factor. Most of his works also were funded by the nuclear industries in the USA, Japan, Sweden, the UK and Taiwan, and by the US Nuclear Regulatory Commission.

## 2.3 Meeting and Collaboration, a Particular Context

Industrial and research community's interest for human factors is nothing new in the mid-1980s. By the 1960s, development of the nuclear industry and modernization of air transport stimulates many research programs (e.g. Swain 1963; Newell and Simon 1972; Rasmussen 1983; quoted by Reason [3]). Researches then were

mostly conducted under the '*human error*' paradigm. The 1980s were marked by a series of industrial accidents (Three Mile Island, 1979; Bhopal, 1984, Chernobyl and Challenger, 1986; Herald of Free Enterprise and King's Cross Station 1987; Piper Alpha, 1988). Investigations following these accidents brought the Safety community to question the understanding of accidents solely based on operator's error. In this scientific, industrial and social context, NATO and the World Bank funded many multidisciplinary workshops on accidents. The first one was held in Bellagio, Italy, 1981. It received the name of "*first human error clambake*".

At Bellagio's Clambake, Reason and Wreathall met. This fortuitous meeting led them to become (in Wreathall words) "*social friends*". Indeed, according Wreathall, "*intellectual communion was quick with Reason but also with other researchers in vogue on the issues of human error at the time. Swain, Moray, Norman*". Reason and Wreathall started corresponding and met at different conferences during the 1980s. Both took commercial projects for industrial groups such as British Airways and US NRC in which they employed each other as professional colleagues. At that time Reason was ending his taxonomy of unsafe acts. He started writing a book on human error aimed to his cognitive psychologist peers. The *Safety Culture Decade* context and choice of reducing first chapter's size brought him into writing a chapter on industrial accidents. Therefore, he intended his book to both the research and the industrial world (he progressively became familiar with thanks to his Wreathall & Co's joint missions as well as others). To communicate his new vision of *organizational* accidents, Reason called on his friend Wreathall to help to design a simple but effective model that would be included in the 7th chapter of *Human Error*. This model was to become, ten years later, the famous SCM.

## 3 Birth and Growth of the SCM

Section 2 has presented the two SCM's fathers, their backgrounds and the context in which they were brought to meet. This section focuses on their collaboration from 1987 (when the writing of *Human Error* begun) to 2000 (publication of the latest SCM version). We first look back at the discovery and exploitation by Reason of the nuclear field (Sect. 3.1). We then explicit the shift that the psychologist made from fundamental to applied research (Sect. 3.2). Section 3.3 is devoted to the percolation of defense in depth into the SCM. Finally, we look at the developments which led the Wreathall and Reason's early accident model, to become, in 2000 the famous and widely used SCM (Sect. 3.4).

### *3.1 Reason, Human Error and NPPs*

In the late 1970s Reason is still far from the nuclear power plant (NPP) control rooms. Yet this industrial field will be one of the most influential for its work. In

1979, the TMI incident operates an awareness of the influence of local workplace conditions on the operator's performance. While Charles Perrow sees in TMI the advent of a *normal accident*, Reason finds the first level of his taxonomy: distinction between *active* and *latent* errors. In 1985, Reason and Embrey publishes *Principles Human factors relating to the modeling of human errors in abnormal condition of nuclear power plants and major hazardous installations*. One year later, the Chernobyl disaster provides an unfortunate case study. Reason introduces a new distinction between errors and violations in his taxonomy. In 1987, he publishes an article in *British Psychological Society* bulletin devoted to Chernobyl errors' study from a theoretical perspective. In 1988, he publishes *modeling the basic tendencies of human operator error*, thus introducing an error model which allows modeling the human behaviour of problem solving (the Generic Error Modeling System, GEMS). Reason's cognitive models were then based on observations in NPPs control rooms as case study of human behavior.

The development of distinction between accidents theories based on active or latent errors and violations, is strongly linked to the development of nuclear energy and its safety culture. From 1979 to 1988, Reason uses accident investigations and gets used to the field and its culture. For all that, his productions remains designed to his peers. A turning point is met when the observation process becomes a collaborative one and that Reason's psychologist work mingles with the engineering one of Wreathall.

## *3.2 From Fundamental to Applied Research*

1987 represents a break in Reason's work [2]. After studying everyday errors for ten years, Reason holds a major contribution to his discipline with the taxonomy of unsafe acts [3, p. 207]. He publishes the *Generic Error Modelling System* ([4] Fig. 1a), a combination of his classification with the *Skill Rule Knowledge* model of Danish psychologist Rasmussen [5]. It presents the types of human failures linked with the specificities of a given activity. This theoretical cognitive model still belongs to the field of psychological research (model quoted 192 times).

The same year, Reason works on a chapter of *Human Error* dedicated to industrial accidents and designed for security practitioners. He has the backing of his friend Wreathall. Reason says he looked for a manner of "*showing people what our work was about*". Wreathall talks in these terms of the genesis of the first model "*during an exchange in a pub (the Ram's Head) in Reason's home town (Disley Cheshire, England), we have drawn the very first SCM on paper napkin. Initially, James saw the organizational accident as a series of "sash" windows opening or closing thus creating accident opportunity*". Wreathall allowed the psychologist to combine his accident theory (resident pathogens metaphor; [6]) and his error taxonomy with a pragmatic model of any productive system.

The shift over, the cognitive and theoretical model changed into a descriptive and empirical one (Fig. 1b). The book *Human Error* received a warm welcome by

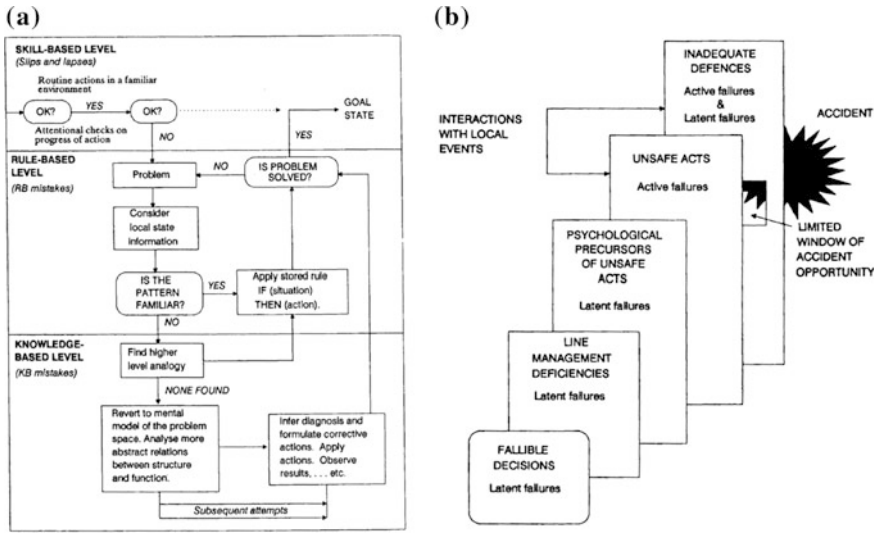


**Fig. 1** Reason's taxonomy backed **a** at the cognitive SRK model by Rasmussen produces a theoretical model; **b** at the Wreathall's productive system's model produces an effective descriptive model

both research and industrial communities (quoted 8604 times). Reason became a Wreathall & Co' director and continued his work related to industries "*he supported psychological dimensions of the reports produced by the firm. As early as 1991* according to Wreathall, *James was familiar with the engineering community and became conductor of the various works made by Wreathall & Co', especially for the American nuclear domain*". Reason will remain a part-time collaborator of Wreathall & Co' and then WreathWood Group until he retired in 2012.

## *3.3 The Defense in Depth Contributions*

The engineer's contribution goes beyond the pragmatic modeling of a productive system. Wreathall's training and experiences with the British submarines nuclear reactor and CEGB NPPs' safety gave him specific defense in depth[1] thinking. When

[1]Early 1960, the military 'defense in depth' concept is introduced into the US nuclear safety policies. It concerns the hardware and construction design (fuel and reactor independent physical barriers containment). The TMI incident extends it to human and organizational dimensions. In 1988, an International Atomic Energy Agency working group publishes an issue entitled Defense in depth in nuclear safety [7] which establishes defense in depth as a doctrine of nuclear safety. Doctrine based on three concepts: barriers (implementation of physical protection systems), defensive lines (structural resources and organizational security), and levels of protection

he designed the first SCM, Wreathall chose a representation of superimposed plates. These plates evokes defense in depth's *levels of protection*. Reason then explains each plate's failure using his taxonomy and understanding of organizational accidents. The *Swiss cheese* nickname and representation is late. Still it's rooted in the first graphical choice. Wreathall's contribution overtakes engineering understanding of a system: it carries the defense in depth thinking.

Defense in depth is clearly mentioned in an early SCM version ([3, p. 208]; Fig. 2a).[2] It incorporates an accidental *trajectory of accident opportunity* which provides information on respective contributions of the psychologist and the engineer. On the left hand, the white plates represent the organizational (managerial level) and human failures (unsafe acts): contribution of the psychologist. On the right hand, gray plates represent defense in depth as a block (set of defenses ensuring the system's integrity): it's the engineer contribution. Human variability may confuse the engineer (which partly explains the historical *human error* understanding of accidents). On the other hand, technical and organizational sides of safety often confuse academic researchers. In the SCM, disciplines collaboration is used to display the complex interactions between humans and technology and therefore, emergent properties of system's security (Fig. 2b). Finally, the differences in graphical complexity between the theoretical and empirical models are to be noted. In the next section, we will argue that the success of the SCM also lies in the choice to simplify the drawing in a heuristics release.

## 3.4 SCM Evolutions

Reason and Wreathall kept working together and using the SCM within Wreathall & Co's reports. A little after 1993 Wreathall suggests replacing "*latent error*" (referring to organizational failures) by "*latent conditions*". This change acknowledges the fact that efficient decision at a given time may have negative outcomes at another time or place in the system but these decisions may not be wrong at the time —they are just made under uncertainty. In addition to these semantic changes, SCM graphically evolves (over 4 times in the 1990s). Its use reached many sectors such as energy or transportation [11]. During 1990s, Rob Lee, director of the Australian Bureau of Air Safety Investigation, suggested representing gaped barriers as Swiss

(Footnote 1 continued)

(arrangement of barriers and defensive lines according to structured objective regarding the potential event's gravity).

[2]If the original version labels defense in depth (Fig. 2a), the 1993 French translation (by an academic) changes the label for «défenses en série» (serial defenses). Loss of sense due to field sensitivities' manifestation.

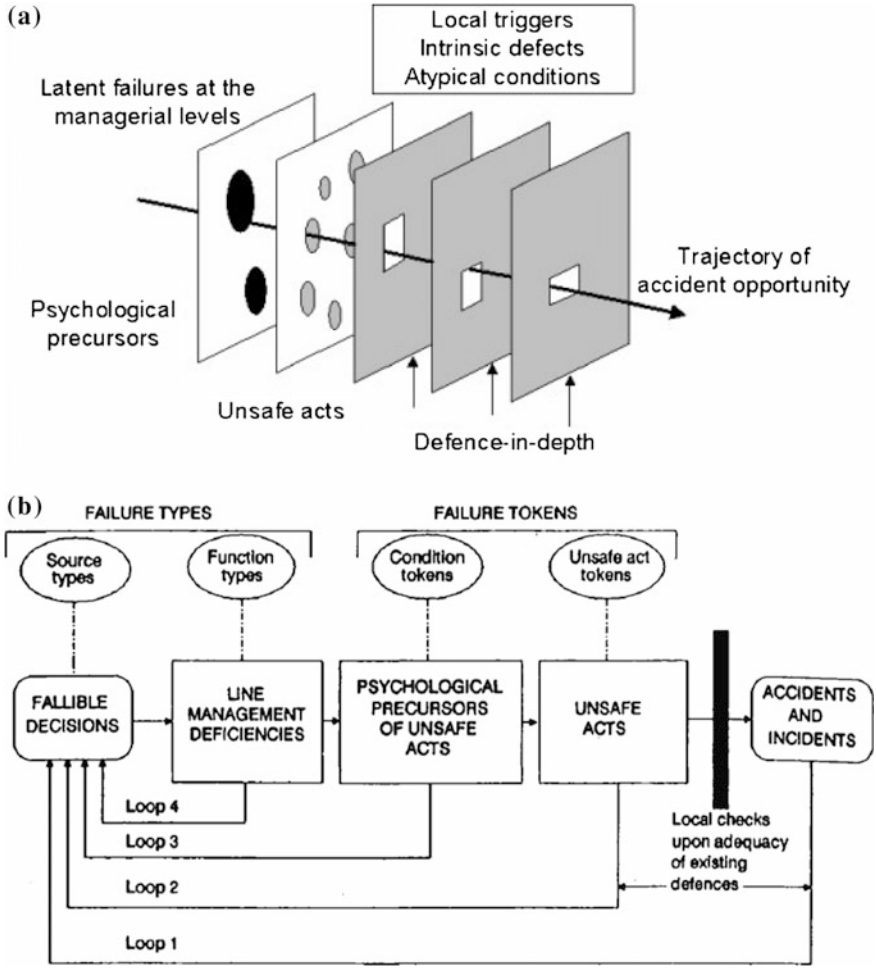


**Fig. 2** **a** The accident causation model published in 1990 explicitly introduced the defense in depth concept. **b** A more complex representation showing the interactions between human and technical dimensions of the system

cheese slices [9]. The idea attracted Reason, then working on a new SCM version for the *British Medical Journal* ([8], Fig. 3). This was a landmark article (quoted 3442 times) and in 2003 Reason was appointed *Commander* of the British Empire for his work on patient safety. The SCM was born. Its simplicity and empirical pragmatism made it the vector of a new paradigm of Safety: *the organizational accident*.

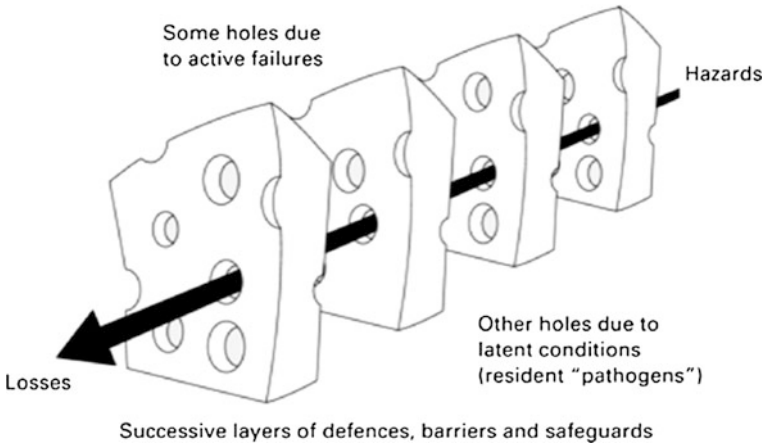


**Fig. 3** SCM version where the cheese slices represent a system's defenses [8]

## 4 Discussion

A detailed study of the SCM is both simple and complex. Simplicity comes from the abundance of sources. This model has been widely quoted and Reason is a prolific author (149 publications; [10]). Complexity arises from the nature of the model's origin: a collaborative and poorly documented work between distinct but interactive worlds, research and industry. Meeting the two fathers of the SCM was a great help, it surely helps preventing from retroactive bias.

This study was guided by intuition that the success of SCM lays (mostly) in its simple graphical representation. If it is undeniable that *Swiss cheese* representation has played a role in the socialization process of Reason's work, it actually seems it has mostly caused theoretical and methodological pitfalls [11]. A second hypothesis was that success of the model was the result of the appropriation of research findings by industry. It emerges that it is more the appropriation of industrial experience by the academics and long term collaboration that gave the SCM its empirical pragmatism, likely to encourage its use and spread. If Reason and Wreathall's meeting was helped by a favorable social and industrial context (Safety Culture decade and human error clambakes), their collaboration stood thanks to a mutual will of convergence. We note the importance of backgrounds and early life experiences that led Reason working in aviation community and Wreathall meeting systemic thoughts and human factors early in his studies. This shared background guaranteed sensitivity and brought a common language to the two: a collaboration prerequisite. Finally, more than simply causing their meeting, the social demand at that time (industry funding many research programs) also allowed the evolutions of the model. Through various research programs and industrial demands, the SCM was used and shaped.

The SCM took time to evolve and meet industrial (and in a way, social) demand. As we tried to demonstrate here, the essence of its efficiency is cross-disciplinary background and collaboration. We must now use these assets as a mean to address extreme situation so one can operate quick, innovative and pragmatic solutions when unfortunately faced with it.

**Acknowledgements** My thanks to Professor Reason for his hospitality, on 7 January, 2014, and to Mr. Wreathall for coming and meeting us at MINES ParisTech Centre of Research on Risk and Crises, on 10 October, 2014. Their answers provided valuable insight to our work. Great thanks to Professor Frank Guarnieri for his unconditional support and precious advices. Thank you to Professor Joonhong Ahn for hosting the International Workshop on Nuclear Safety: *From Accident Mitigation to Resilient Society Facing Extreme Situations*, at the University of Berkeley, California, March 2015.

## References

1. F. Guarnieri, S. Travadel, Engineering thinking in emergency situations: A new nuclear safety concept. Bulletin of Atomic Scientists **70**(6), 79–86 (2014)
2. J. Larouzee, F. Guarnieri, D. Besnard, *Le modèle de l'erreur humaine de James Reason*. Papiers de Recherche du CRC, MINES ParisTech, 44 pp. (2014)
3. J. Reason, *Human Error* (Cambridge University Press, 1990)
4. J. Reason, *Generic error-modelling system (GEMS): a cognitive framework for locating common human error forms.* New Technol. Hum. Error **63** (1987)
5. J. Rasmussen, *Skills, rules, and knowledge; signals, signs, and symbols, and other distinctions in human performance models.* IEEE Trans. Syst. Man Cybern. **SMC-13**(3) (1983)
6. J. Reason, *Resident pathogens and risk management*. W.B. Workshop Safety Control and Risk Management (1988)
7. INSAG, *Defense in depth in Nuclear Safety.* International Nuclear Safety Advisory Group Report (INSAG) IAEA (1996)
8. J. Reason, Human error: models and management. BMJ **320**(7237), 768–770 (2000)
9. J. Reason, E. Hollnagel, J. Paries, *Revisiting the "Swiss Cheese" Model of accidents*. ECC No. 13/06 (2006)
10. J. Larouzee, F. Guarnieri, *Fond bibliographique Sir James Reason – une vie dans l'erreur.* Papiers de Recherche du CRC, MINES ParisTech, 12 pp. (2015)
11. J. Larouzee, F. Guarnieri, *Huit idées reçues sur le(s) modèle(s) de l'erreur humaine de Reason*. Revue d'Electricité et d'Electronique (2014)