General Conclusion

Designing and developing a systemic safety model requires the acquisition of background knowledge related to control and systems theories. Thus, the concepts of systemic, control, control loop, feedback, etc. must be fully understood, which in turn requires a good understanding of the concepts belonging as much to the 'systemic' domain as the safety domain. This dual understanding of the 'foundations' raises many questions:

- What is a system? How should it be understood?
- What is complexity?
- What are the different types of systems?
- What is a dynamic system? What is feedback?
- What is dynamic behaviour?
- What is safety? What is a safety system process?
- What is a hazard analysis technique?
- How can analysis techniques be integrated into the life cycle of a system?
- What is a hazard? What is an accident?
- What is the triptych that makes up a hazard analysis approach?
- Etc.

However, a good knowledge of the safety and systemic domains is insufficient to exploit systemic accident models: the latter require that their user has an intimate understanding of their challenges, which goes far beyond applying safety principles in a given system. It is rather a matter of understanding a system in which safety is an emerging property, and therefore to highlight a complementarity between a level of safety and a systemic optimization.

Nowadays, it is accepted that systemic accident models can overcome the limitations of traditional models based on the analytic approach, which has proved to be

F. Guarnieri, E. Garbolino (eds.), *Safety Dynamics*, Advanced Sciences
and Technologies for Security Applications,
https://doi.org/10.1007/978-3-319-96259-7

inadequate for dynamic systems. The first, so-called linear, accident models were only able to provide 'stable' solutions and predict four types of unstable situations:

- stable oscillations, i.e. slight variations of the system, that can be brought back into balance by linear and proportionate responses;
- exponential growth oscillations, i.e. systemic behaviour characterized by positive and growing feedback loops, and negative loops that can 'cushion' variation;
- asymptotic stability, characterized by negative feedback loops that make it possible to achieve a goal or stabilize a system;
- unlimited growth, characterized by positive feedback loops leading to exponential growth.

One of the advantages of linear accident models is their ability to provide accurate predictions about the future state of a system, while systemic accident models can only provide one law governing the evolution of a system. However, the dynamics of system, and sociotechnical systems are nonlinear. To understand an 'accident' system, in the context of a linear accident model, it is sufficient to model it by examining its behaviour when it is at steady state. Once this modelling is done, it is then possible to predict the general behaviour of the system when the initial conditions are known. However, these linear accident models are only valid and really appropriate when the system is in a situation that is close to a stable equilibrium.

Systemic accident models, based on general system theory and control theory, focus on the analysis of a system that is in a steady state and evolving towards an accidental state. As soon as information concerning the elements of the system is known, it becomes possible to describe its dynamic behaviour, to analyse it, or to carry out an accident investigation. In other words, as soon as the initial conditions of a dynamic system are known, it is possible to describe its trajectory and the law governing its evolution.

Systemic accident models are thus able to produce types of solutions that are different to those described by traditional accident models, while leaving room for structural changes. They also make it possible to propose ways to reinforce the robustness of a system, i.e. its sensitivity to small disturbances in order to keep it in a 'safe' state.

In this context, a systemic accident model, such as the STAMP model, seeks to reinforce the robustness and stability of a system in the face of disturbances. Two types of stability exist in a dynamic system: dynamic and structural. Dynamic stability is translated by a system behaviour in the face of a disturbance that is exterior to the system (for example, an external 'noise'). In this context, the system will seek to provide a response that is adapted to an external signal while maintaining a 'safe' state. Structural stability (which is at the heart of the STAMP model, with the establishment and study of a hierarchical structure) concerns the control of the structure (composed of a large number of elements in nonlinear interaction). This structural stability remains internal to the system and the maintenance of a 'safe' state depends on the capacity of the system to maintain internal control over its structure.

Systemic accident models have therefore been developed to take into account the complexity of sociotechnical systems. In much of the literature, complexity is synonymous with a large number of interactions between elements. This condition is necessary but not sufficient. In practice, a system can be composed of a large number of interactions, but lack any sign of complexity (for example, an ice cube, which is composed of a large number of molecules in linear interaction, is in a state of stable equilibrium). The additional condition for characterizing complexity is the notion of nonlinearity. In this case, a system composed of many elements in nonlinear interaction can be considered as a complex system. This is the case for sociotechnical systems.

As has been discussed throughout the book, systemic accident models are based on Bertalanffy's general system theory.[1] In this context, they study systems that are in (or close to) a state of stable equilibrium (when they are subject to disturbances). However, complex systems are never in a state of stable equilibrium, and it is therefore not particularly useful to attempt to study them as complex systems with tools that are based on a theory that studies systems that are in (or close to) a stable equilibrium.

This contradiction underlies the STAMP accident model.

The STAMP accident model is based on two theories: system theory put forward by Ludwig von Bertalanffy, and control theory, notably the work of Norbert Weiner on the concept of feedback. These theories set out the characteristics of systems described in the framework of classical science—the notions of equilibrium, linear causality and negative feedback. These notions make it possible to explain the context in which accident models have developed.

The notion of equilibrium corresponds to the state of a system when it automatically corrects deviations from its trajectory determined by basic laws. In this context, a sociotechnical system is a set of systems in which the natural state is a stable equilibrium where any deviation is attenuated or corrected by negative feedback. When a disturbance is too great and does not allow the return to the initial equilibrium state, the system can migrate to a new state of equilibrium.

Linear causality postulates that there is a direct link between the cause acting on a system and the changes in the structure of the system, in other words, cause and effect are proportional.

Finally, the notion of negative feedback, found in the work of Newton, Darwin or Bertalanffy translates a mechanism that exists when a system departs from its equilibrium, due to external disturbances or fluctuations that are inherent in its dynamic, and which attenuates their effects to allow the system to return to its initial equilibrium state. The notion of negative feedback has largely inspired the field of cybernetics.

Accident models are therefore developed to describe, interpret and predict an accident. Here, the accident model approach is based on a deterministic approach, which constitutes the basic principle of any prediction. In practice, the fundamental objective of an accident model is predictive; it focuses on the analysis of hazards in

[1] Please see : Von Bertalanffy, L. (1968). General system theory. *New York*, *41973*(1968), 40.

a system (static or dynamic, linear or nonlinear) in order to prevent behaviours that can migrate a 'safe' system to an accidental state. All accident models have been designed with the aim of understanding and prediction in different types of systems, such as physical or sociotechnical systems. Linear accident models are limited, and represent an approximation of reality that is only useful when the system is close to a stable equilibrium state. However, an accidental phenomenon never occurs when a system is close to a stable equilibrium. These accident models have been built on a deterministic process, combining an analytical and a systemic approach (now considered complementary). They have always assumed that the studied systems are 'integrable' (linear) and deterministic. However, systems such as sociotechnical systems integrate many elements that interact nonlinearly, generating many types of behaviours and therefore changes.

A consequence of this is that systemic accident models take account of the notion of 'time'. At present, the modelling of sociotechnical systems is based on the theory of integrable dynamic systems, in other words, systems that are close to a stable equilibrium state, in which (ongoing and never-ending) time flows. In these systemic accident models, the system is dynamic and evolves over time. However, a systemic accident model that studies a dynamic system in stable equilibrium state cannot be made to evolve continuously, because any response to a disturbance can only be 'linear'. A system, whatever it may be, in a state of stable equilibrium cannot evolve, because its trajectory is a fixed point that does not move. A stable equilibrium state is only governed by linear processes and does not drive the system to change. A system only evolves in a state of instability based on irreversible processes. It then becomes difficult to speak of dynamics and evolution over time, as defined in the framework of Bertalanffy's general system theory, in the context of systems in an unstable equilibrium—as is the case for sociotechnical systems.

Time is a parameter that imposes itself on any system. It must be considered as a degree of freedom, or even as an emergent property, and not as a universal parameter imposed by default on any system. The physical laws that general system theory is based on do not distinguish between the future and past directions of the 'arrow of time' in a non-integrable dynamic system. However, this notion of the arrow of time makes perfect sense in the theory of non-integrable dynamic systems.

Thus, time (notably, the arrow of time[2]) emerges from the instability and irreversibility of processes. Entropy is born out of irreversibility, which is non-existent in a state of stable equilibrium. The arrow of time emerges from instability and nonlinearity; it is a source of phenomena such as self-organization and evolution. From this perspective, changes within a sociotechnical system do not appear at the end of a given period of time, but as the arrow of time appears, as it emerges from nonlinear processes within a non-integrable dynamic system. In other words, the notion of the arrow of time becomes 'meaningful' in irreversible processes.

[2] Please see Prigogine, I. (1984). Order out of chaos: Man's new dialogue with nature and Prigogine, I. (1980). From being to becoming: Time and complexity in the physical sciences.

Consequently, the very evolution of a system is its ability to draw out its arrow of time, passing through a state of unstable equilibrium and therefore, nonlinearity. This arrow of time is a driving force and constitutes a source of change within the very structure of the system. Thus, it only exists in existence, in other words, only following the appearance of irreversible processes leading to change and evolution, unlike a classical approach where 'time' appears before any ongoing, never-ending existence.

The evolution of a sociotechnical system does not, therefore, rely upon an ongoing, never-ending 'time' factor, as could be defined when using a modelling tool based on the Bertalanffy's general system theory. A sociotechnical system generates its own arrow of time, characterized by nonlinear and irreversible phenomena that highlight a break in the symmetry. Time only takes on a 'meaning' because a sociotechnical system is a complex system. Thus, the stability (even the safety) of a sociotechnical system can be obtained by modifications to its structure in a given context, in other words, by irreversible processes in response to a given context.

Systemic accident models consider time as a parameter that has no influence on the studied system. However, we have just seen that it is during the emergence of this arrow of time, in a state that is far removed from the equilibrium, that a system can build its own safety-oriented structure. But that is another story, for a completely different book!

Index

F. Guarnieri, E. Garbolino (eds.), *Safety Dynamics*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-319-96259-7