Advanced Sciences and Technologies for Security Applications

Franck Guarnieri · Emmanuel Garbolino
Editors

Safety Dynamics

Evaluating Risk in Complex Industrial Systems

Springer

Advanced Sciences and Technologies for Security Applications

The series Advanced Sciences and Technologies for Security Applications comprises interdisciplinary research covering the theory, foundations and domain-specific topics pertaining to security. Publications within the series are peer-reviewed monographs and edited works in the areas of:

- biological and chemical threat recognition and detection (e.g., biosensors, aerosols, forensics)
- crisis and disaster management
- terrorism
- cyber security and secure information systems (e.g., encryption, optical and photonic systems)
- traditional and non-traditional security
- energy, food and resource security
- economic security and securitization (including associated infrastructures)
- transnational crime
- human security and health security
- social, political and psychological aspects of security
- recognition and identification (e.g., optical imaging, biometrics, authentication and verification)
- smart surveillance systems
- applications of theoretical frameworks and methodologies (e.g., grounded theory, complexity, network sciences, modelling and simulation)

Together, the high-quality contributions to this series provide a cross-disciplinary overview of forefront research endeavours aiming to make the world a safer place.

The editors encourage prospective authors to correspond with them in advance of submitting a manuscript. Submission of manuscripts should be made to the Editor-in-Chief or one of the Editors.

More information about this series at http://www.springer.com/series/5540

Franck Guarnieri • Emmanuel Garbolino
Editors

Safety Dynamics

Evaluating Risk in Complex Industrial Systems

Springer

Editors
Franck Guarnieri
MINES ParisTech/PSL
Research University, CRC
Sophia Antipolis Cedex, France

Emmanuel Garbolino
MINES ParisTech/PSL Research
University, CRC
Sophia Antipolis Cedex, France

ISSN 1613-5113 ISSN 2363-9466 (electronic)
Advanced Sciences and Technologies for Security Applications
ISBN 978-3-319-96258-0 ISBN 978-3-319-96259-7 (eBook)
https://doi.org/10.1007/978-3-319-96259-7

Library of Congress Control Number: 2018957612

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

General Introduction

The formal study of 'systems' emerged in the nineteenth century, with the birth of industry; around that time, work began to appear of the safety and security of these same systems. Faced with the growing complexity of industrial systems, the modern concept of the 'system' began to be formulated, in various scientific fields, from the second half of the twentieth century.

There are many pioneers, and here we will list only a few:

- Ludwig von Bertalanffy (1901–1972), the Austrian biologist, whose book *General System Theory* has become a reference[1]
- Norbert Wiener (1894–1964), the American mathematician who applied system theory to control and communications[2]
- Claude Elwood Shannon (1916–2001), American mathematician and telecommunications engineer[3]
- Warren Sturgis McCulloch (1898–1969), the American neurophysiologist who broadened his research to mathematics and industrial engineering[4]
- Finally, Jay Wright Forrester (1918–2016), American engineer and professor at Massachusetts Institute of Technology (MIT), who developed the application of system theory to industrial dynamics and who created *system dynamics* at the end of the 1950s, a mathematical modelling technique that makes it possible to understand and analyse the so-called 'complex' problems

Forrester has made a particularly significant contribution. His work and publications have been very well received:

---

[1] von Bertalanffy L. 1969/1998. *General System Theory*. George Braziller: New York

[2] Wiener, N. (1948). Cybernetics. *Scientific American*, 179(5), 14–19

[3] Shannon, C. (1949). Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28 (4): 656–715

[4] McCulloch, W. & Pitts, W. (1943). A Logical Calculus of Ideas Immanent in Nervous Activity. *Bulletin of Mathematical Biophysics*. 5 (4): 115–133

- In *Industrial Dynamics*[5] (1961), he describes, with the help of system dynamics, industrial cycles.
- A few years later, he published *Urban Dynamics*[6] (1969) which attracted the attention of urban planners at a global level and led him to meet and join the prestigious Club of Rome.[7]
- From these enriching, productive discussions, he gave us the book *World Dynamics*[8] (1971), which addresses the modelling of complex interactions in the economic, demographic and environmental spheres.

The field of safety studies, like many other domains, could not escape the promise and proven usefulness of system dynamics. In this respect, the work of Jens Rasmussen[9] has had widespread impact. His model makes it possible to study a system by considering its hierarchical structure and dynamic aspects. The integration of dynamics represents a clear turning point in the analysis of accidents and at-risk sociotechnical systems; it allows both negative and positive feedback to be taken into account, thereby creating unique and nonlinear behaviours. Safety becomes a question of 'relations'.

Relations between ideas and concepts (risk, vulnerability, resilience, etc.), between subsystems (prevention, crisis management, feedback from experience, etc.), between man and machine, between organizations (notably in the context of relations between controllers and those they control), etc. It also requires understanding that safety is both organized and organizing. When a company, an institution or a nation produces safety, its constituent elements also act retrospectively on the actions of the entity that created it, by initiating and developing constraints or, on conversely, by creating synergies between subsystems that are constantly changing. Finally, it requires accepting that safety is a potential that actors re-examine and reassess on an ongoing basis, as a function of their needs and hopes, from the point of view of the dynamics and potential of other actors in a given system. This never-ending dynamic can lead to repositioning, evolution, splits and even breaks.

These ideas are generally accepted and therefore widely shared, both within the scientific community and among safety practitioners. However, it is clear that system dynamics has made very few contributions to safety for a very long time. It was not until the work of Professor Nancy Leveson at MIT, a worthy successor to Jay Forrester, that we finally had access to, in the early 2000s, some solid theoretical

---

[5] Forrester, J. W. (1997). Industrial dynamics. *Journal of the Operational Research Society*, 48(10), 1037–1041

[6] Forrester, J. W. (1970). Urban dynamics. *IMR*; Industrial Management Review (pre-1986), 11(3), 67

[7] The Club of Rome, established in 1968, is a think tank made up of scientists, economists, national and international officials, as well as industrialists, who are concerned about the complex problems facing all societies, both industrialized and developing.

[8] Forrester, J. W. (1971). *World Dynamics*. Wright-Allen Press

[9] Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*, 27(2), 183–213

foundations, a robust methodology and a toolbox for modelling and simulating complex systems[10] (notably thanks to software such as Vensim, AnyLogic, etc.).

Leveson designed and developed a model for risk analysis and accident prevention called STAMP (Systems-Theoretic Accident Model and Processes). The clear, underlying hypothesis of this model is that safety is an emerging property of the system and only exists through the presence of interactions between elements and the application of controls within the system's hierarchical structure (a reference to the work of Rasmussen). Leveson's model therefore represents a radical paradigm shift, as the accident is no longer seen as the result of a chain of events (as is found, e.g. in the Heinrich model[11]) but as the consequence of a control problem within the system.

System dynamics makes many promises. Contrary to popular belief, it is not intended to replace any other forms of modelling nor does try to be more detailed, more precise, more efficient, more effective, etc. Its primary purpose is to invite us to look differently at the world around us. A world that is complex only because we decided it would be. Complexity is not actually a state but an attempt to better describe, understand and share the new knowledge that is acquired through a sustained effort to acquire and formalize data and knowledge in order to produce, present and discuss a result that takes the form of a model.

A model that, through its design process, is in no way a black box but, on the contrary, is an artefact, represented with the help of a diagram, in which it is extremely easy to identify the constituent hypotheses, the descriptive variables and the relations that link them to each other.

The diagrammatic representation greatly facilitates decision-making, in that it offers many new points of view that feed into an evolutionary, iterative and ongoing process. Therefore, even if the model helps to produce imperfect 'decisions', its purpose is to be, at each iteration, better understood and more widely shared. In other words, what is sought is not so much the quality of the choice, as the quality of the process that leads to the agreement to decide. Therefore, the aim is no longer to find the best solution but to be equipped with ways to best manage the uncertainties of the situation in question, examined jointly. To improve the quality of decision processes, the system dynamics approach seeks to clarify and share the viewpoints that led to the modelled situation. It draws upon a dynamic perception of the decision-making process, in which, in particular, the scientific-technical point of view represents only one option, among many others, and which is not assumed to be an accurate perception that the decision must aim towards. The objective is not, therefore, the very ambitious goal of producing decisions and definitive results but that of enriching the decision-making process, whether in technical terms (information, the technical quality of actions undertaken, etc.) or with respect to its sociological aspect (more consultation, giving actors greater power in decisions, etc.).

This book has two aims. The first is to return to the main concepts of system dynamics, put forward a theoretical and methodological framework and describe

[10] Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*. MIT Press

[11] Heinrich H. W. (1931). *Industrial accident prevention: a scientific approach*. McGraw-Hill

rigorous approaches to the formalization of models that are designed to understand and simulate sociotechnical systems. The second is to present some actual industrial case studies, which serve as a basis to illustrate and discuss the applications of theories and methodologies based on data that has been collected from partner companies in the chemical, oil and gas and waste treatment sectors.

This book is structured into two main parts.

The first part is subdivided into two:

- The first, Chap. 1, introduces the concepts of *systems*, the *systemic approach* and *systemic modelling*.
- The second is broken down into three chapters that provide details of the actual implementation of dynamic systems according to the work of Jay Forrester. Chapter 2 shows how STELLA software contributed to the modelling of a chlorine storage facility and its associated risks. Chapter 3 describes the modelling and simulation of human, technical and organizational dimensions in the context of an industrial plant, using Vensim software. Chapter 4 focuses on modelling safety behaviours.

The second part is also subdivided into two:

- The first presents, in Chap. 5, the STAMP accident model and the associated analysis tools: STPA (Systems-Theoretic Process Analysis) for hazard analysis and CAST (Causal Analysis based on STAMP) for accident analysis.
- The second is composed of three chapters that describe operational implementations of STAMP, STPA and CAST: Chap. 6 presents an application to hazardous contaminated sediments; Chap. 7 describes an application to offshore oil installations; and Chap. 8 outlines an application to the hazards associated with the Capture, Transport and Storage of CO_2 (CTSC).

The book ends with a conclusion summarizing the contributions and limitations of the approaches and case studies. Finally, it proposes some avenues for future research.

Contents

1 The Systemic Approach: Concepts, Method and Tools 1
Emmanuel Garbolino, Jean-Pierre Chéry, and Franck Guarnieri

2 Systems Dynamics Applied to the Analysis of Risk at an Industrial Installation 31
Emmanuel Garbolino, Jean-Pierre Chéry, and Franck Guarnieri

3 System Dynamics Applied to the Human, Technical and Organizational Factors of Industrial Safety 93
Hafida Bouloiz and Emmanuel Garbolino

4 Modelling and Dynamic Analysis of Safety Behaviour 107
Hafida Bouloiz and Emmanuel Garbolino

5 Stamp and the Systemic Approach 123
Karim Hardy and Franck Guarnieri

6 Using Stamp in the Risk Analysis of a Contaminated Sediment Treatment Process 151
Karim Hardy and Franck Guarnieri

7 Contribution of the Stamp Model to Accident Analysis: Offloading Operations on a Floating Production Storage and Offloading (FPSO) 179
Dahlia Oueidat, Thibaut Eude, and Franck Guarnieri

8 Systemic Risk Management Approach for CTSC Projects 197
Jaleh Samadi and Emmanuel Garbolino

General Conclusion 223

Index 229

Chapter 1
The Systemic Approach: Concepts, Method and Tools

Emmanuel Garbolino, Jean-Pierre Chéry, and Franck Guarnieri

The advent of the systemic approach heralded a turning point in the history of science and its application to the organization, and to production. The approach, which considers phenomena and problems as systems, only really began to distinguish itself from the classical analytical approach in the mid-twentieth century, but its origins are much older. The *systemic* approach, as it is currently called, can be considered as a general scientific paradigm, such as the Matter of Life or Society. It offers a generic way to construct and present valid, relevant and rational representations of the most diverse, changing situations. The general system theory, which was conceived by von Bertalanffy (1968), encapsulates these ideas and entails a theoretical and practical method: modelling.

This chapter presents the main principles of the systemic approach. It focuses on the evolution of related concepts, the principal types of models and, more specifically, dynamic modelling. It also presents some examples of the contribution of systems thinking to industry, in particular from the angle of system dynamics.

E. Garbolino (✉) · F. Guarnieri
MINES ParisTech/PSL Research University, CRC, Sophia Antipolis Cedex, France
e-mail: emmanuel.garbolino@mines-paristech.fr; franck.guarnieri@mines-paristech.fr

J.-P. Chéry
AgroParisTech, Montpellier, France
e-mail: jean-pierre.chery@teledetection.fr

F. Guarnieri, E. Garbolino (eds.), *Safety Dynamics*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-319-96259-7_1

1.1 The System and the Systemic Approach

The word *system*, which generally means "assembly", derives from the Greek verb *systeo,* a word that was used to denote the action of attaching elements together. In systems thinking, authors define their own interrelationship between elements, as illustrated in Durand (2006, pp. 7–8) who offers the following examples:

- "A set of units in mutual interaction" (von Bertalanffy);
- "A set of elements in dynamic interaction, organized around a goal" (de Rosnay);
- "A global unit made up of interrelationships between elements, actions or individuals" (Morin).

If the system is considered as an object of knowledge, it can be defined, after Le Moigne (1977), using three characteristics (see Fig. 1.1):

- The *ontological* pole refers to what the object *is*. It considers the system in terms of its elements, and its boundary with its environment. This defines the system's structure, i.e., all of the *a priori* stable relationships between the elements.
- The *functional* pole refers to what the object *does*. This is clearly linked to the nature of the system, and therefore the ontological pole. From the theoretical point of view, the functional aspect is characterised by goals. Beyond consideration of what the system does, it also addresses what the system is *for*. Artificial systems, such as machines or robots,[1] are designed and built by humans. These artificial or technical systems can be easily identified. They have little capacity for change: their goal is clear and defined by their designers. It is more difficult to identify the purpose of open (e.g., living) systems, which raises philosophical and spiritual questions, such as "What is the meaning of life?" In this context, it becomes important to distinguish between the function and purpose of a system,

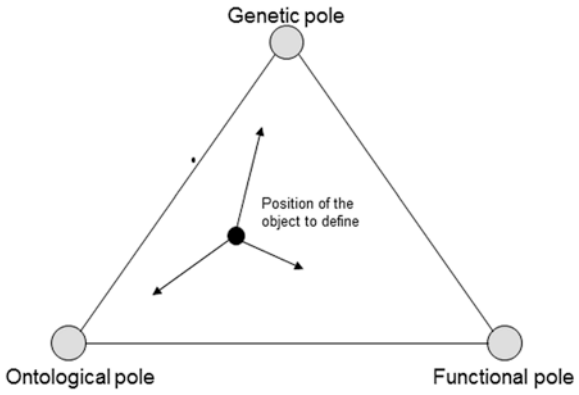

Fig. 1.1 Definition of the object of study using a triangulation based on the poles "Genetics", "Ontological" and "Functional". (Following Le Moigne 1977, p. 39)

[1] The concept of the artificial system extends beyond the boundaries of the finished object: beyond the machine or robot, there is the human designer.

or its *means* and its *ends*. In general, complex systems have multiple ends: potential contradictions arise when trying to satisfy incompatible goals or objectives.
- The *genetic* pole refers to what the object *becomes*. The system is observed over time, and considered to have the capacity to re-define itself over time. From this point of view, memory, history, trajectory and dynamics are system attributes.

The following section looks at the development of systemic thinking in the West, and compares it to analytical thinking.

1.1.1 History

Western scientific thought became autonomous between the late fifteenth century and the twentieth century with the rise of rationalism. It incorporated the scientific heritage of antiquity and medieval thinking in the Mediterranean, through various intermediary countries (Egypt, Greece, Persia, India, and the Arab-Muslim world). In the West, the constitution of a socially-recognized body of scientists, supported by an increasingly specialized body of engineers, emerged in the seventeenth century. It was at this time that Descartes proposed a scientific approach that shattered the scholastic tradition, which was increasingly considered to be obsolete in light of the great Copernican and Galilean discoveries. The words of the Bible could no longer provide an explanation for everything, and it became necessary to construct a method that met the new need for intellectual rigour. In his *Discourse on the Method*, Descartes (1637) outlines four precepts that underpin the analytical approach: doubt and certainty; the division of problems into as many parts as possible; the assembly of simple objects; and completeness.

Analytical thinking postulates that everything is the sum of its parts; likewise, a general explanation is made up of a set of individual explanations. This provided the foundation for one of the key currents of scientific thinking that describes the world. The nomenclature claims to be exhaustive and exclusive: anything can be categorised into only one category, and be placed in a hierarchy of other categories. In the eighteenth and nineteenth centuries, this approach gave rise to taxonomy and systematics in the life sciences, formalized by Carolus Linnaeus (Encyclopaedia Britannica, online Internet site).

However, analytical thinking was not the only school of scientific thought during the long period of Western imperialism. For example, in his posthumous *Thoughts,* Pascal (1670), expressed the holistic thinking that is at the heart of systemic approach.

"Since everything then is cause and effect, dependent and supporting, mediate and immediate, and all is held together by a natural though imperceptible chain, which binds together things most distant and most different, I hold it equally impossible to know the parts without knowing the whole, and to know the whole without knowing the parts in detail."

This quotation indicates the need for an overall vision. Everything has properties that cannot be reduced to the sum of the properties of its parts. This line of thought is characterised by Pascal's firm religious beliefs that support the notion of the divine.

Earlier Greek authors, such as Heraclitus, held atheist beliefs (Patrick and Bywater 2014). For Heraclitus, access to the totality is considered through the union of opposites, their coexistence and co-production: "living in their death and dying in their life". The opposition does not require an explanation based on causal exclusivity—linear causality—and narrow system ontology. Heraclitus also poses the problem of identity, or the ontology of objects, with the famous phrase "Into the same river you could not step twice", which raises the issue of permanence, conservation vis-à-vis dynamics, time and changes in appearance.

It is not until the early twentieth century that the failure of analytical thinking to provide adequate answers becomes apparent. It is faced with a growing body of knowledge that is scattered across highly compartmentalized disciplines in an academic structure that is, on the one hand, inherited from encyclopaedism and, on the other, from the positivism of Comte. This is illustrated by the synopsis of his *The Course in Positive Philosophy* (*Cours de Philosophie Positive*) in 1826 (Le Moigne 1990, pp. 154–155).

The first criticism of the analytical approach or, rather, the first suggestions that another view of the scientific process was possible appeared at the dawn of the twentieth century. Changes were seen during the first third of the century: in physics, with the rise of thermodynamics and its implications for industry; in evolution, in population growth research in biology; and in the use of iterative calculation in differential equations. The issues that were raised in the first half of the twentieth century addressed the notion of different states, potential or realized, and the role of this difference in processes. Wiener and von Bertalanffy (Durand 2006) were important contributors to the founding of a new scientific approach—cybernetics and systems science in the 1940s.

In biology, von Bertalanffy's work does not require the separation of bodies in order to differentiate them, in a dissection-like process. The isolation of organs or the accuracy of microscopic descriptions is not enough to explain what a living organism is. Moreover, the Darwinian revolution of the late nineteenth century launched the search for explanations in terms of relationships between organisms and their environment, their habitat and their population in competition with other types. The emergence of genetics, in the early twentieth century, suggested that living organisms have physico-chemical properties that act as non-material information. In biology, the emergence of new forms of multicellular organisms—from an initial cell, for example—required going beyond the analytical method.

In order to try to understand the contribution of systems theory, de Rosnay (1975) compared the characteristics of the analytical approach and the systemic approach (Table 1.1).

Table 1.1 Comparison of analytical and systemic approaches (After de Rosnay 1975)

Analytical approach	Systemic approach
Isolates	Unifies
Nature of interactions	Effects of interactions
Precise detail	Global perception
One variable at a time	Groups of variables
Reversible phenomena	Duration and irreversibility of phenomena
Validation by experimental proof	Validation through modelling and simulation
Precise and detailed models	Global templates
An efficient way to handle linear and weak interactions	An efficient way to handle nonlinear and strong interactions
Teaching by discipline	Multidisciplinary education
Detailed action programme	Action through objectives
Knowledge of details	Knowledge of goals

As with any beneficial innovation--and, in science with an improved understanding of phenomena—adoption was gradual. The systemic approach was taken up over several decades by other disciplines, countries, research networks and application areas (industry, management, information technology, engineering, etc.).

One particularly interesting contribution of the systemic approach is its contribution to the development of interdisciplinary research. As it connects the components of a system, it can be used to study a system as a whole. It highlights emerging behaviour, and the fact that systems can be seen as a methodological support that links the knowledge, expertise and data from various disciplines relating to the same system. Consequently, industrial risk management has become an interdisciplinary activity: engineers took an interest following the emergence of dependable systems in the 1920s. Since the late 1980s it has integrated approaches and tools from information technology, ergonomics, psychology and sociology—as can be seen in the pages of international journals such as *Safety Science*, *Risk Analysis*, and the *Journal of Loss Prevention in the Process Industries*.

The role of the systemic approach is to define the means of prevention and protection in response to industrial hazards. Despite the lack of methodological developments, there are some examples. The Method Organized for a Systematic Analysis of Risk (MOSAR) procedure was designed in the late 1990s (Perilhon 2003) and is based on modelling the industrial system and a two-level risk analysis. The macroscopic analysis examines the main elements in proximity to each other (operators, hazardous materials, at-risk processes, etc.); and the microscopic analysis explores the technical and operational faults previously identified using traditional dependability methods. The approach proposed in this book is similar to MOSAR, but here the behaviour of the industrial system is studied dynamically, i.e., the evolution of the system's elements and its general behaviour are examined over time.

The following section completes this brief history by presenting the key concepts of systems thinking.

1.1.2 The Main Concepts of the Systemic Approach

Durand (2006) identifies four major concepts that characterise the systemic approach:

- interaction
- comprehensiveness
- organization
- complexity.

These are described below.

Interaction is related to causality in a system: elements interact, i.e., they perform actions on other elements and are subjected to actions by other elements. When one element does not interact with any others, possibly because it only performs or receives one action, it is considered to be external to the system. The systemic approach offers the advantage of diagnosing the causal relationships that describe an element's reflexivity: the action of element *A* on element *B* affects the nature or intensity of the action of *B* on *A*. This feedback occurs in many natural and artificial systems. It can be energetic, material or informational depending on the type of system.

Comprehensiveness reflects the notion that everything cannot be reduced to the sum of its parts. There are specific properties that depend on the subset of the system in question or the entire system. These irreducible properties change depending on the degree of aggregation of elements, or subsets of elements of a system: the hierarchy of the aggregate elements reflects these qualitative or quantitative changes in recognized properties. It is important to include them in the study of a system.

Organization refers to the consideration of both the structure and operation of a system. Typically, the arrangement of the system's components assures its functions and processes. These functions and processes are differentiated in such a way that the elements that make them effective constitute the actual structure of the system. Organization implicitly suggests, in common parlance, a goal. This is generally the case for most artificial and social systems, in the production of goods or services, for example. However, the organization of natural, open systems is a poorly understood aspect that science seeks to explain. For example, zoogamy—the pollination of flowering plants by animals such as insects—is an *organization* of the reproduction of these plants that shows that the *plant system* is open to other living species. The establishment of control within the organization cannot be understood using the simple analogy of a closed, artificial system. To achieve the unalterable goal (if it can be identified) of reproduction, the phenomenon of inter-species symbiosis has to be established.

In economics, the comparison of *intra*-enterprise performance based on an integrated model, and *inter*-enterprise performance based on a decentralized model—such as the *industrial district*—leads to a debate about the modalities of controls in exchanges between the system (the organisation) and its environment, and its ability to achieve its purpose when the system is very open. In risk management, the imple-

mentation of a safety management system to monitor subcontractors, for example, is an additional organizational means of control between the company and its socio-economic environment. This safety element, which is typically organizational, is necessary because of the interactions between the company and its contractors; these exchanges can generate failures that can lead to accidents.

C**omplexity** must be distinguished from the term *complicated*. A complicated system consists of many elements, and the multiple relationships make it difficult to understand. The end result, however, may be a simple, stable, repetitive cycle that runs like clockwork. The analytical approach can be used to understand this complicated system. Generally, a complicated system has linear causalities, little interactive causality and is unlikely to be open to its environment. There are several properties or characteristics of complexity, however, that can be observed in some systems (Zwirn 2006):

- Self-organization: the ability of a complex system to change its organization without any causal influence from its environment;
- Emergence: the emergence of new and dynamic system properties, characterized by the concepts of phase transition and percolation.

Other properties (such as the system's sensitivity to conditions or constraints on its subsequent dynamics and its adaptability) demonstrate complexity. Generally, complexity suggests that it is difficult to predict the dynamics or evolution of a system (Donnadieu and Karsky 2002). Complexity can be viewed as "uncertainty in richly organized systems" (Morin 2005, p. 49).

Unpredictability can be reduced by taking into account those elements that were initially excluded from the system, but which are subsequently found to have strong causal relationships with those items that were initially included in the system. The aim is to take better account of a system's spatial complexity—*spatial* in the sense of the structural relationships between elements—by extending the system's boundaries. Another aspect of unpredictability which is very difficult to reduce, relates to the system's temporal dynamics. Certain temporal phenomena (dependent on the system's spatial complexity) produce events that can create bifurcations in the system dynamics.

These four major concepts that underpin the systemic approach reflect the difficulties of studying, understanding and acting on natural and artificial systems. One method that can be used to assess, diagnose and understand these types of system is systemic modelling.

1.2 Systemic Modelling

Modelling a system involves constructing a representation of the system—a model—that simplifies, at least in part, its structural and functional properties. The representation seeks to maintain, as far as possible, intelligibility, reliability and usefulness. Several categories of system models can be identified.

1.2.1 The Major Categories of Models

Research in systems modelling has led to systems being classified in several different ways. One example, based on the level of organization of systems, defines nine levels that constitute what Boulding (1956) calls the *general system*. These levels are represented, in increasing order of complexity, by: (i) the frameworks (the static structure); (ii) clockworks (a simple dynamic system); (iii) the thermostat (the control mechanism, or cybernetic system); (iv) the cell (the open system, or self-maintaining structure); (v) the plant (the genetic system, differentiated functions); (vi) the animal (the decisional system); (vii) the human (an intelligent system that is able to imagine, interpret symbols, etc.); (viii) social organization (socio-cultural system); and (ix) transcendental systems (systems that exceed the capacity of human knowledge to understand, but which humans can question).

Based on his modelling method and a re-reading (and adaptation) of the work of Boulding (1956), Le Moigne suggested (1977, 1983 pp. 128–149) that an organization can be made up of the following new levels:

1. The passive, unnecessary object: these objects are what they are, they are considered in their entirety by the modeller. They include, for example, atoms, planets, stars, cells, words in isolation, an alarm, a valve, an operator, etc.
2. The active object: the object moves and can act on its environment, other objects, etc. For example, the planets move around the sun, the latter's gravity acting on the former. This activity does not change the nature of the object. The activation of an alarm does not change its nature or the elements of the system, but may trigger some of them to react.
3. The active and regulated object: determinism suggests that its behaviour appears to be related to initial conditions. Similarly, its behaviour is regulated by control loops that give it stability. For example, the activation of an alarm triggers a servo valve to close, and in turn, the alarm stops.
4. The object is aware of itself: the object is open to its environment and communicates with it to maintain itself in a stable condition. Here, information becomes an element that links the object with the world around it. The object perceives, and can represent its environment. Leakage sensors positioned around a storage system provide electronic devices with information that can activate or deactivate an alarm, if needed.
5. The object decides what it does: the object demonstrates an internal logic that drives it to make decisions, based on a goal, as a function of its perceptions and environmental constraints. Systems that are serviced and controlled by software can be activated as a function of changes in environmental parameters.
6. The active object has a memory: this memory is closely associated with the decision-making process that integrates the representation and information flows in its environment. Le Moigne uses this to introduce memory processors that are linked to decision-making processors. Computer-based control systems used in industry can record information captured by sensors and interpret it. For example, software can anticipate thermal runaway in a chemical reactor.

7. The active object can coordinate: here, it acquires the ability to coordinate its activities given the information available to it. Some robots are able to work independently in an extreme environment to gather information on the state of a system.
8. The active object can imagine and self-organize: the object has the ability to generate symbolic information that may not be directly related to the information it perceives. It can develop a new logic that the decision processor can use to adopt a new behaviour. This level is characterized by the emergence of intelligence. The operator or group of operators is able to organize and adapt to a new situation—for example crisis management on an industrial site.
9. The active object can autofinalise: the object is able to formulate projects, for itself, its entourage or its environment. This level equates to the emergence of consciousness (self-awareness) in relation to the environment (the object's place in the world around it). Any at-risk industrial project is found at this level as the decision-making process is based on multiple criteria (economic, environmental, ecological, social, etc.).

Le Moigne's proposed control system consists of the finalization system, the intelligent system and decision-making system. This control system interacts with the information system and the operating system.

More recently, Durand (2006) adopted a different perspective, and developed a taxonomy of models based on how they are used:

- The *cognitive model* is a simplified representation of the system, which focuses on the system's knowledge. Typically, cognitive models use graphs and pure analogue forms such as symbols. An ellipse can be used to represent the path of the Earth around the Sun, for example, where the line represents the path of the planet around its star that, in simple terms, cannot be departed from. Similarly, in industry, Piping and Instrumental Diagrams (PIDs) are used to provide a simplified view of the systems implemented in a process; and in dependability, the Bow-Tie risk analysis method provides a simplified graphical representation of the occurrence of a dangerous phenomenon and its impact on the system, the environment and health.
- The *decision model* is a decision-making tool that is typically used for optimization. The decision to be made is expected to be the best possible in a given context. Usually, decision models seek, through simulation, to represent the different consequences of decisions. They then use computer programs based on combinatorial and probability principles. The modelled system exhibits equal-end properties, i.e., given different initial conditions (e.g., initial decisions), the system reaches the same end state. This shifts the choice of the decision from the goal to be achieved, to the cost of reaching that goal (some decisions are more expensive than others). Software packages that can simulate dangerous phenomena play a role in decision making in urban planning and crisis management, for example, through the definition of safety perimeters.
- The *normative model* focuses on establishing parameters to monitor, maintain or achieve, depending on the state of the modelled system. This model focuses on

human and artificial technical systems. A normative model can only focus on the structure of the system or its operation. Normative models may reflect the organization or management of an economic activity, typically a business. Activities that pose risks (threaten the safety of people, property or the environment) in some industries can be identified using models that set safety rules. Threshold limits are established that must not be exceeded, such as the maximum load or concentration of a product in physical and chemical processes; at the same time humans monitor system performance and take appropriate action (e.g., alert procedures and backups). Most accidents occur because the normative model was either poorly designed or poorly applied. In the latter case, it may still be argued that the model was poorly designed, in that it did not take appropriate account of the elements that caused the problem.

- The *predictive model* can produce information that indicates the future state of the modelled system, including in abnormal or unusual conditions. Generally, the predictive model's design uses a dynamic representation of the system in an appropriate past, and present timeframe. From this representation of the structure and the past operation of the system, the (typically computerised) model reports trends in the system state or in scenarios that change the system's dynamics, which provide an understanding of its sensitivity. Given the ever-increasing power of computing technology, predictive models are implemented as increasingly sophisticated computer programs. These models can be deployed in monitoring tools in the chemical industry, for example, where they can be used to anticipate the likelihood of a thermal runaway so that appropriate preventive actions can be taken.

These categories of models are not mutually exclusive. The modelling approach aims to increase understanding, improve reliability and enhance usefulness of the system. It produces a model that reflects these properties. Generally, *a minima*, all models are cognitive: the system that an actor seeks to act upon, to set rules for, or to predict its future, must first provide a representation of itself that expresses the state of its knowledge. In industry, the categories of models that are used depend on the particular system being studied. The codified representation of a given industrial plant or its principle elements (buildings, flows, production tools, control equipment, safety systems, etc.), for example, is simultaneously a cognitive model and a normative model. Similarly, official documentation, such as plans of the industrial facility, typically reflects both of these aspects of modelling.

An industrial plant can also be represented by a decision model that incorporates knowledge of risk factors and accidents, along with the *a priori* actions that need to be refined when these factors recur. The decision model draws upon information produced by the cognitive and normative model, and helps to define the available choices and actions. The predictive model is typically used to simulate particular scenarios. It can be used to characterize the spatial and temporal extension of phenomena and events. Normal production flows and accidents (including effects such as the severity of a gas leak, and the concentration and diffusion of a toxic substance in the atmosphere) can be simulated in different contexts.

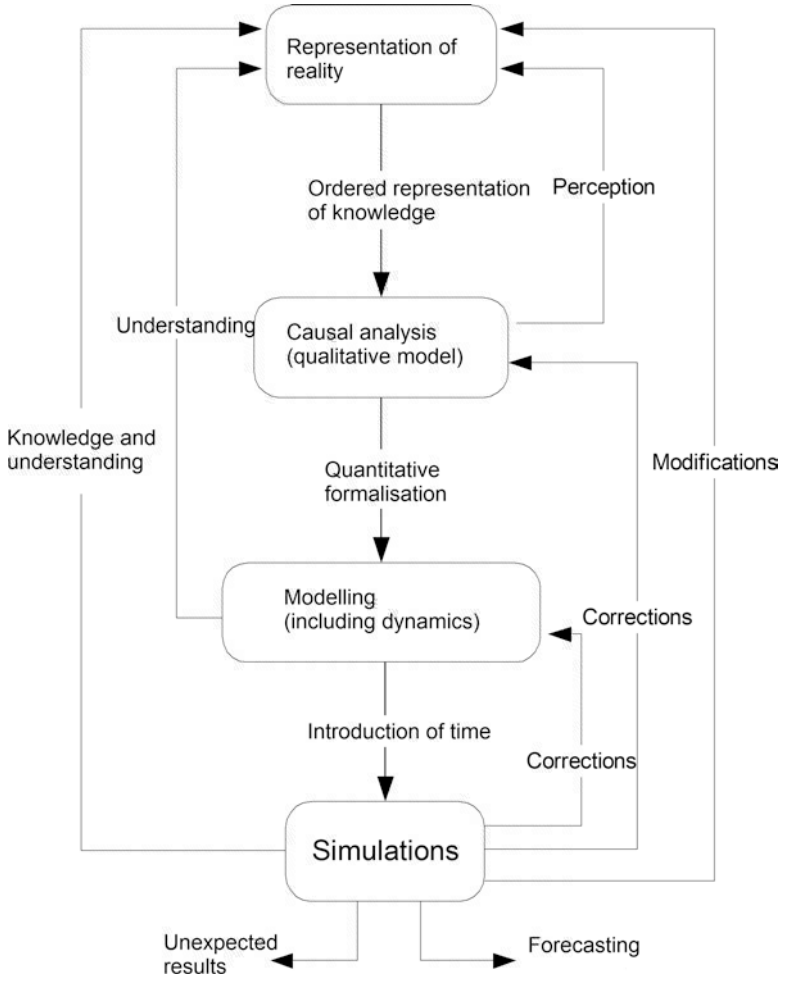

Fig. 1.2 The construction of a simulation model. (Translated from Donnadieu and Karsky 2002, p. 120)

These interrelated categories of models result in relatively elaborate system models, such as those developed for simulation. The foundations for these models are typically found elsewhere, and expressed formally in ways that are understandable and can be shared. The construction of a simulation model iterates between a representation of reality, which may initially be very simple or shared, and simulations that are the results of using a model that is based on the identification of causal phenomena (Fig. 1.2).

The dynamic risk analysis approach (presented in Chap. 2) is inspired by this system modelling approach and the simulation of system behaviour. The proposed simulation model should not be constructed on the assumption of the production of

a stable, permanent tool that is defined once and for all, and which is used (unmodified) for forecasting when the need arises. The purpose of a simulation model is linked to the needs of a given project at a particular time. As time passes, the actual system is modified as a result of the lessons that are drawn from the model and applied to the organization and its procedures. This makes the model out of date and potentially inaccurate. Modelling is a process of creating and updating a model that satisfies the current needs and constraints. A *good* model should therefore be considered as one that is based on a specific methodology: it is reproducible and stable, adaptable and robust, and can be revised based on the results of the model simulation.

The dynamics of the model can become complex and counterintuitive as the number of system elements and their interactions increase. This makes it harder to determine the probable evolution of the system under particular conditions. Systemic modelling, which aims to produce simulations, addresses the system properties that are the basis of this complexity. The use of modelling methods makes it easier to understand systems, through the transcription of systemic phenomena from their expression as theoretical concepts to practical modelling tools. The rest of this book focuses on the system dynamics method.

1.2.2 System Dynamics: A Modelling and Simulation Method

In his *Industrial Dynamics* book, Forrester (1961) defines system dynamics as "a way of studying the behavior of industrial systems to show how policies, decisions, structures, and delays are interrelated to influence growth and stability." This requires the identification (through a graphical representation) of causal chains that define the evolution over time of a given system's components. These causal chains form feedback loops, which identify the processes that underlie counterintuitive phenomena using computer simulations. The graphical representation of feedback loops between elements of the system is called a *causal graph*. Most software packages used for developing simulation models provide a visual representation, in the form of a graph or a stock-flow diagram, which defines the system's elements as a function of their causal interactions. One such software package, STELLA®, is discussed in Chap. 2.

Forrester (1961) explains the detailed procedure for constructing models, which consists of five main steps:

- identify the key variables that continuously describe the status of the system's components in interaction;
- develop a hypothesis that may explain the dynamic behaviour, with a view to the proposed formalization of the system that distinguishes it from its environment;
- develop a formal model of the causal relationships between variables, based on knowledge and hypotheses, and identify feedback loops;

- decompose the causal phenomena, using a top-down approach, to understand complexity at the point where it affects dynamics;
- present these relationships in the form of differential equations in a mathematical framework that can be used in simulations.

System dynamics provides a way to study, model and simulate the processes that lead to changes in, or the maintenance of natural and artificial systems over time. These changes (if they occur) are observed when digital or ordered values are used as signals in the system being studied.

Forrester's method has been widely adopted, and has inspired many prospective models. Perhaps the most famous of these is found in the Meadows Report for the Club of Rome, entitled *Dynamics of Growth in a Finite World* (1974). The report's conclusions forecast the collapse of the world's population due to declining natural resources, increased pollution levels in the twentieth century and the depletion of non-renewable energy resources. The report educated industrialists and governments about the risks of uncontrolled growth.

The variables used in the Meadows Report relate to the demographics of the global human population, the overall level of pollution, the use of natural resources, the extent of farmland, etc. The report influenced the idea of sustainable development that was introduced in the late 1980s in the report of the World Commission on Environment and Development. A new edition of the Meadows Report was published in 2004, which confirmed some of the results from the original version.

The Meadows Report showed that the world's population could be stabilised through: birth control; the protection of resources and nature; limiting industrial emissions; and the conservation of arable land. The application of system dynamics to the study of the dynamics of the global population has led to the formalization of a model (World 3) that can represent the most significant variables. This approach can also be used to simulate the system's behaviour and explore different scenarios by varying its parameters. Some of these variations are political choices: the approach therefore contributes to the implementation of a decision support framework.

The application of system dynamics in industrial safety is designed to provide a formal decision support framework for industrialists. This framework is specific to the implementation of prevention and protection measures for workers, facilities, local residents and the environment.

Systems theory has also been combined with control theory to create the Systems-Theoretic Accident Model and Process (STAMP; Leveson 2004a, b). Unlike traditional accident models, which consider that accidents are the result of a chain of failures, the STAMP model adopts a systemic view of accidents (Leveson et al. 2003; Leveson 2004a, b; Leveson and Dulac, 2005; Stringfellow Herring et al. 2007). Industrial systems that have been studied using the STAMP method are based on a dynamic process that seeks to continuously adapt, by responding to internal and external changes to the system, in order to achieve their objectives. Safety is therefore considered as an emergent property of a system, and becomes a control problem that can be solved by strengthening safety constraints. These con-

straints do not apply directly to the system's elements but are imposed in the context of rules that define the interaction *between* these elements. Consequently, in the STAMP model, accidents result from a lack of control, or the improper application of safety constraints during the system's design, development and operational phases. From a systemic point of view, accidents are therefore the result of poor feedback that fails to provide a level of safety that corresponds to the optimal performance of the industrial system (an inappropriate or the lack of a recovery loop).

The basic concepts used in systems dynamics are described below. These provide the foundations for the work described above, and for the study of the industrial system that appears in Chap. 2.

1.2.2.1 Systemic Concepts in System Dynamics

System dynamics can be characterised using the following concepts (Donnadieu and Karsky 2002):

- state and force
- feedback loops
- nonlinearity
- deadlines; and
- structural change

These concepts are illustrated below, using a case study of a chlorine unloading unit that is used in the synthesis of plastics.

State and Force

A dynamic system can be understood in terms of its past and expected future changes. These changes are evaluated through a comparison of (null or actual) values at two points in time; these values continuously record the state of system elements. Changes in state are the result of interactions between elements. The direction of change in the value of a particular element depends on the values of the other elements with which it has a direct relationship. If the values of those other elements cancel each other out, the element does not change state; if there is a net change in values (non-null), the element changes state. These change values are referred to as *forces*.

The state of a chlorine stock (Cl_2) at the current time depends on the state at a particular previous point in time, and the forces—chlorine feed and consumption—that act on the state between the two time instants. This concept is reflected in the term *stock–flow*, which indicates this view of the state and the forces at play in a modelled system.

The relationship between an element and the other elements that act upon it via different forces is, from the systemic viewpoint, a circular causality. It is represented by a feedback loop as a function of the principle of the interaction.