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