# Modelling and Hazard Analysis for Contaminated Sediments using STAMP model and STPA tool

Karim Hardy, Franck Guarnieri

Journal of Energy and Power Engineering 7 (2013) 496-500

# Modelling and Hazard Analysis for Contaminated Sediments Using STAMP Model and STPA Tool

Karim Hardy[1] and Franck Guarnieri[2]

*1. Center for Catastrophic Risk Management, Haas Business School, University of California, Berkeley CA 94720, USA*

*2. Center for Research on Risk and Crisis, Mines ParisTech, Sophia-Antipolis 06904, France*

Received: April 26, 2012 / Accepted: August 08, 2012 / Published: March 31, 2013.

**Abstract:** The goal of this article is dual: first, introducing a new model of accident named STAMP (systems-theoretic accident modeling and processes); then applying the model to an innovative process for the treatment of contaminated substances and the re-use of treated substances. This article is a demonstration for a need of a new tool to take into account hazards and safety within socio-technical systems.

**Key words:** Model of accident, safety engineering, environment, contaminated substances, re-use.

## 1. Introduction

Processes for remediation (removal of pollution or contaminants) of contaminated sediments have become very efficient. These technologies, which are particularly complex, call for a comprehensive approach to risk analysis which characterises all threats (to humans, equipment, local residents, the environment etc.). The STAMP (systems-theoretic accident model and processes) accident model is an example of such a comprehensive approach, and it has been chosen to characterise the risks associated with Novosol®, an innovative remediation process. Risk analysis is carried out through the application of STPA (STamP-based Analysis).

This following presentation is organised into four sections. The first describes the Novosol® process for treating contaminated sediments. The second introduces the STAMP accident model, together with the associated technique STPA (which can be used both to evaluate safety and to perform accident analysis). The third section describes the concrete application of the STPA technique to the Novosol® process. The fourth section is the conclusion.

**Corresponding author:** Karim Hardy, research scholar, research fields: safety engineering, reliability, risk management within organizations. E-mail: khardy@cal.berkeley.edu.

## 2. The Problem of Contaminated Sediments and the Novosol® Process

The natural environment is subject to many forms of industrial, urban and agricultural waste, which create a rich and diverse sediment contaminant. Solvay SA began development of Novosol® in partnership with the Université Libre de Bruxelles [1, 2] in 1993. It was initially developed to treat airborne ash resulting from incineration. From 1999, it was applied to the treatment of a wide range of contaminated sediments.

Novosol® is divided into two stages [3]: a stage of phosphatation, which aims to stabilize the heavy metals present in the sediment, followed by a stage of calcination, which destroys organic matter and provides reusable materials.

This technology, which brings together many stakeholders, creates a high level of risk which must be controlled. Control is achieved through the application of a risk analysis technique known as STPA. STPA is based on the STAMP systemic accident model which

advocates that the socio-technical system be considered in its entirety [4, 5].

## 3. The STAMP Model and the STPA Technique

STPA is based on the three concepts just described, and can be used for safety assessments or accident analysis. It is implemented in three main phases described below:

- Phase 1: defines the safety requirements of the system. It is divided into two sub-phases. The first sub-phase defines requirements in terms of safety. The second establishes the safety control structure, which defines the roles and responsibilities of system components, and aims to identify all interactions between them;
- Phase 2: integrates the safety requirements of the system, in the form of safety constraints, at each hierarchical level in the structure;
- Phase 3: process models (control loops) are formalised. This is in order to identify any weak controls which may lead to the violation of a security constraint, and consequently a state in which an accident can occur. The controls and constraints defined in Phase 2 are potentially subject to violations arising from the process models and control loops inherent at each level of the structure. Consequently, the objective of this third phase is to determine at which level of the process model, and where in the control loop, there are weaknesses which may cause the violation of a constraint. Constraint violations can make the system shift towards a state where an accident may happen.

## 4. Application of the STPA Technique to Novosol®

Each of the stages of the STPA methodology is now reviewed and applied to Novosol® [5]:

- Phase 3.1: definition of system requirements with respect to safety and control structures

Using the STPA method, the requirements and the "system" constraints of Novosol® are defined in the first sub-phase. Table 1 shows the requirements and constraints for businesses currently using Novosol® (comprising Solvay SA during development, and currently SEDISOL and SIFA).

The cornerstone of this sub-phase is to define and to establish the control structure for system safety, as described by Leveson [6, 7]. Using the definition of requirements and constraints from the first sub-phase, a hierarchical control structure can be created (Fig. 1) which includes a definition of the roles and responsibilities of each component—in terms of both control and feedback.

The analysis provides an overview of the system, and highlights interactions between the hierarchical levels. Using this structure, roles and responsibilities are integrated, and it becomes easier to determine the influence components have on each other. Establishing roles and responsibilities support the following phase: the definition and integration of constraints, at the level of each structural component.

- Phase 3.2: integration of system requirements at each level of the hierarchy, in the form of safety constraints

This second phase depends on the first. It aims to integrate requirements and safety constraints, with respect to the various interactions between components, at each hierarchical level. Requirements are defined, and then applied (in the form of safety constraints) to the interactions between components of the safety control structure (identified in Phase 1). Constraints must be analysed in detail. It is at this point that inadequate constraints, which could play a role in creating an accident, are identified.

The result of this analysis translates into the definition of inadequate, or (in the framework of a security assessment) potential control measures. Inadequate controls are identified at each hierarchical level, which correspond to the interactions identified when the control structure was prepared (Table 2).

**Table 1 Examples of requirements definition and constraints for businesses operating Novosol®.**

| Business using Novosol® (SEDISOL or SIFA) |
|---|
| Safety requirements and constraints |
| Treatment of sediments contaminated by organic compounds and heavy metals |
| Responsible for the smooth conduct of inspections and preparation of reports on the use and development of Novosol® in consultation with national and international bodies |
| Responsible for defining requirements and the operational performance of Novosol® with respect to national and international regulations |

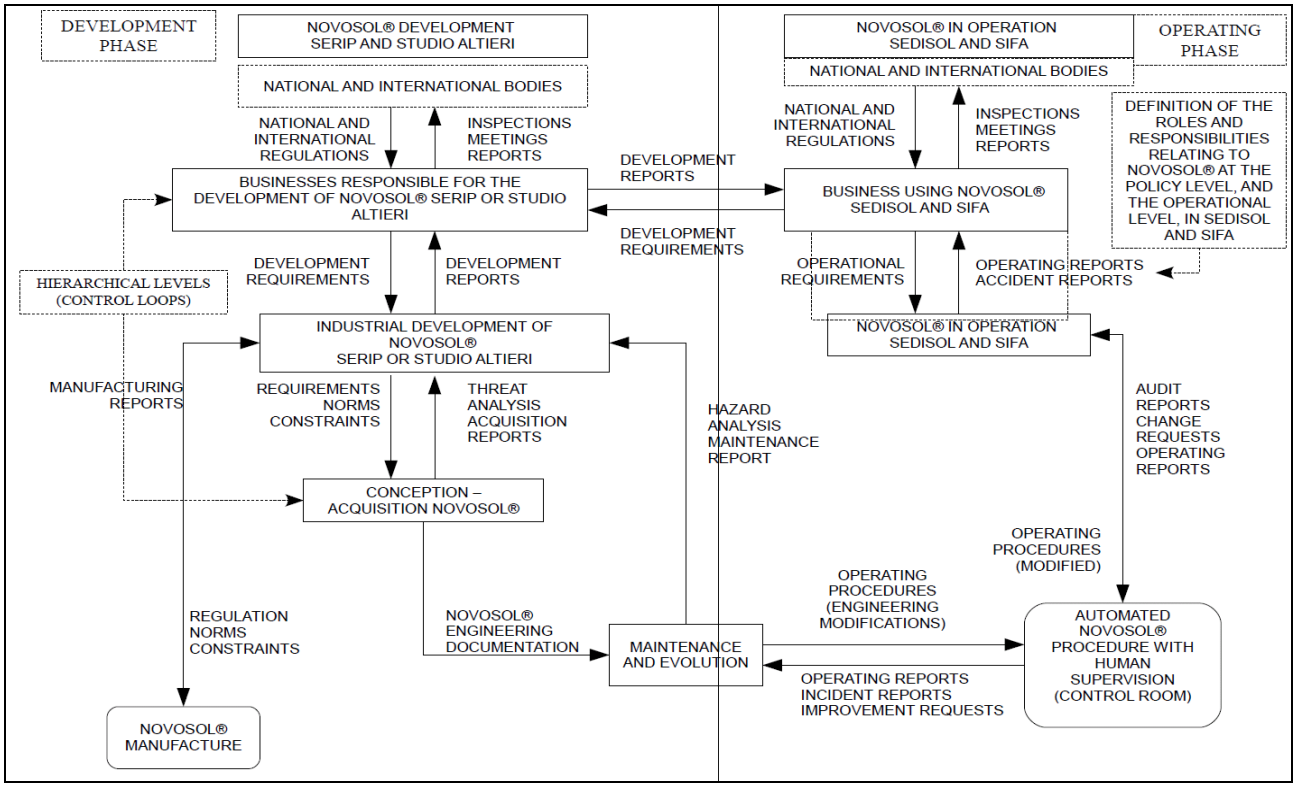


**Fig. 1 An analysis of novosol® using the stpa technique, the structure takes into account the development and operation of novosol®, and shows the interactions between hierarchical levels [5, 8].**

**Table 2 Inadequate control mechanisms for businesses using Novosol®.**

| Business using Novosol® (SEDISOL or SIFA) |
|---|
| Potential or inadequate control measures |
| The operating company does not meet operational requirements for the safe use of Novosol® |
| The operating company is not able to meet the requirements of the company responsible for the development of Novosol® |
| The operating company does not provide inspection reports to overseeing agencies |

Inadequate control mechanisms are translated into constraints and safety requirements then integrated at the level of the system component (Table 3).

Phase 3.3: Analysis of the process models (control loops (Fig. 2)) to identify weaknesses in control that could lead to the violation of a safety constraint and therefore a state where an accident could occur

The constraints defined in Phase 2 can be violated, and shift the system towards a dangerous state where an accident may occur. The objective in Phase 3 is to determine where in the control loop (or loops) a weakness (or weaknesses) may surface, as it is these weaknesses which lead to inadequate controls and change the state of the system.

As an example, Fig. 3 describes the “maintenance and evolution” control loop of the system.

**Table 3 Potential constraints for businesses using Novosol®.**

| Business using Novosol® (SEDISOL or SIFA) |
|---|
| (Potential) constraints |
| The operating company must be able to meet safe operating requirements |
| The operating company must be able to meet the developmental requirements of Novosol® |
| The operating company must provide inspection reports to overseeing agencies |

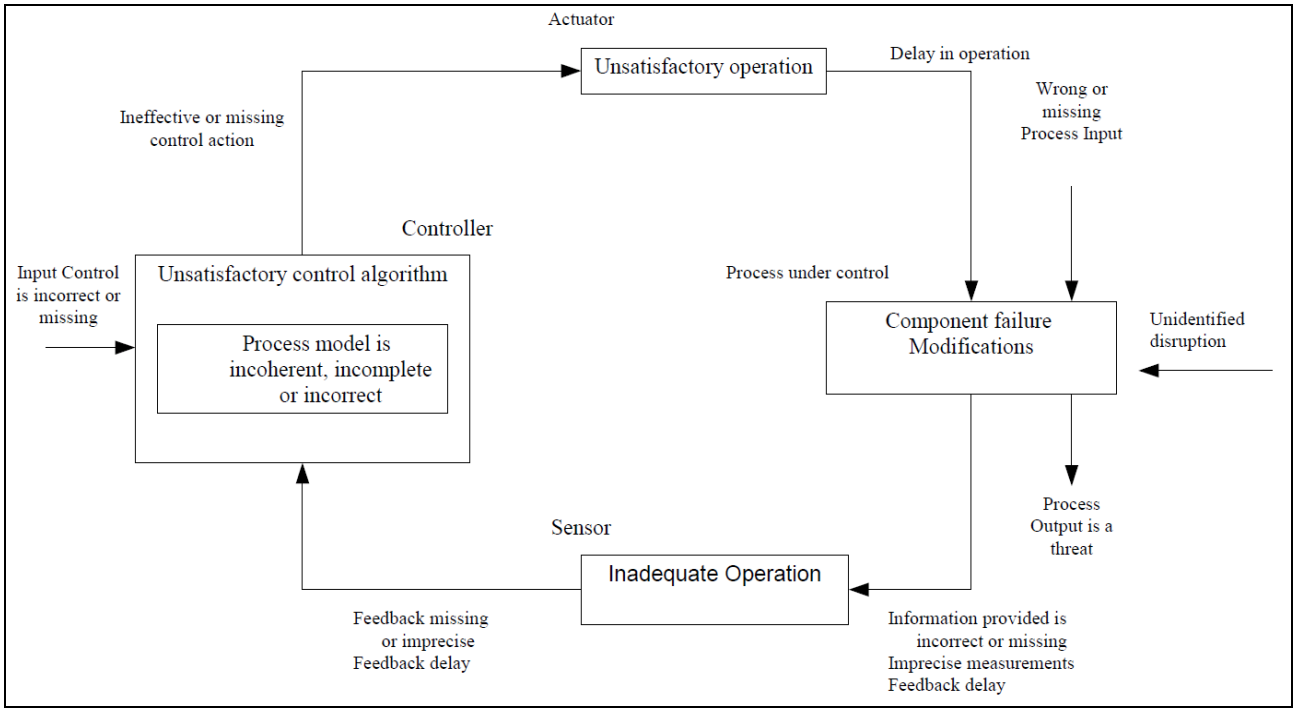


**Fig. 2 Defects in the control loop, finding weaknesses in a control loop enables inadequate control actions to be identified.**

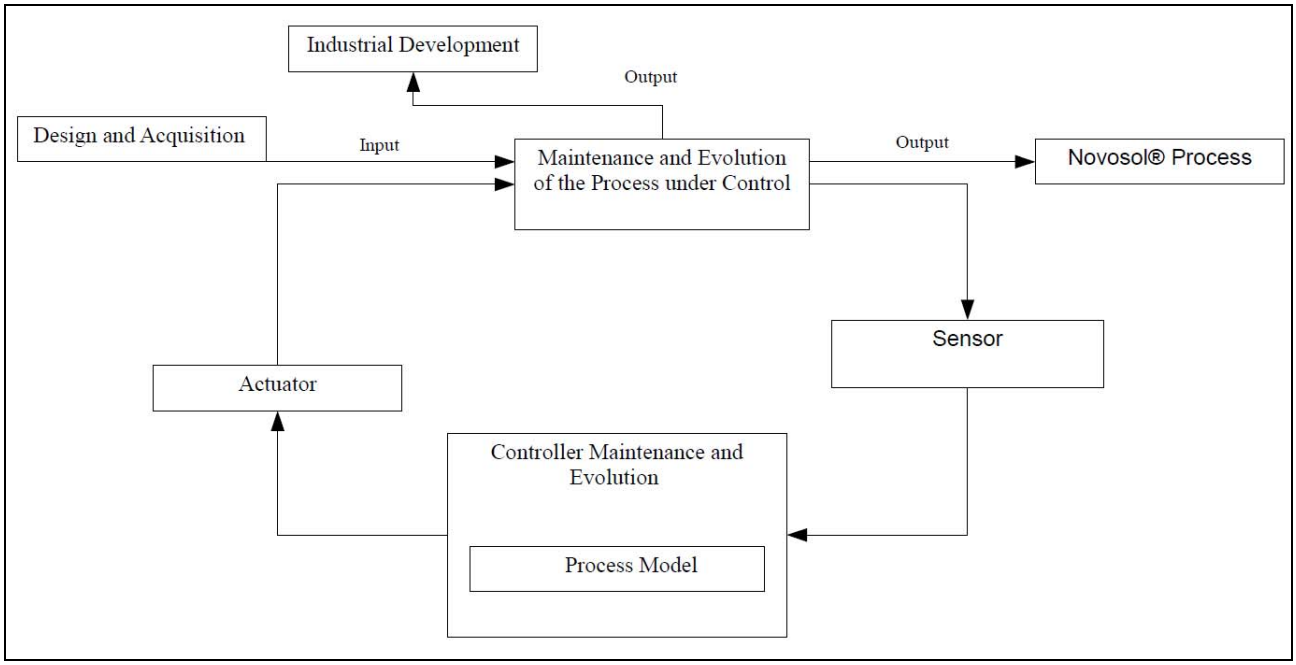


**Fig. 3 The "maintenance and evolution" control loop of Novosol®, this loop integrates the various components which interact with the process model at a particular level, it highlights interactions at various hierarchical levels.**

## 5. Conclusions

The STPA technique, based on the STAMP model, allows to consider a system throughout its life-cycle, taking into account all possible interactions. It focuses not on a chain of events, but on the problem of control between different hierarchical levels of the system. The clear advantage of its application to Novosol® is that it is possible to establish an overall view of the system, and not simply to focus on the technical process. This generates an optimisation of both the treatment process, and the safety and performance of the system as a whole.

## Acknowledgments

The authors wish to thank:

• Solvay S.A. and especially Guy Depelsenaire for funding this research. Solvay S.A. is a Belgian chemical company with two major sectors of activity: chemicals and plastics;

• ANRT (National Association of Technological Research), for providing a grant to carry out this work. ANRT is a French research and development non-profit organisation (including both public and private sector businesses) which aims to optimise innovation and research in France;

• The MIT (Massachusetts Institute of Technology) and especially Nancy Leveson (Complex Systems Research Laboratory), for hosting me for six months in order to conduct research on the STAMP model. The Complex Systems Research Laboratory is headed by Professor Nancy Leveson who is responsible for developing the STAMP model.

## References

[1] D. Breugelmans, Novosol®: The Story of a Pluridisciplinar Step by Step Approach, Environmental Research and Development, Annual Novosol® Seminar, Brussels, Belgium, 2007.

[2] G. Depelsenaire, Novosol ®: Stabilization Process for Mineral Residues Contaminated with Heavy Metals and Organic Compounds, Annual Novosol® Seminar, Brussels, Belgium, 2006. (in French)

[3] S.A. Solvay, Novosol® Home Page, http://www.novosol.be (accessed Feb. 22, 2011).

[4] K. Hardy, The system safety discipline: A response for safe innovative technologies, a case study, in: International Symposium on Sediment Management, Lille, France, 2008.

[5] K. Hardy, Contribution to the study of a model of systemic accident, case of STAMP model: Implementation and suggestions for improvement, Ph.D. Thesis, Center for Research on Risk and Crisis, Mines-ParisTech, France, 2010. (in French)

[6] N.G. Leveson, A new approach to hazard analysis for complex systems, in: International Conference of the System Safety Society, Denver, CO, United States of America, 2003.

[7] N.G. Leveson, A new accident model for engineering safety systems, Safety Science 42 (4) (2004) 237-270.

[8] K. Hardy, Towards a development of safe innovative systems: Integrating health and safety at work, in: Conférence Lambda Mu 16, Avignon, France, 2008. (in French)