Modelling and hazard analysis for contaminated sediments using stamp model

Karim Hardy, Franck Guarnieri

HAL Id: hal-00614418

https://minesparis-psl.hal.science/hal-00614418

Submitted on 10 Jan 2013

Modelling and Hazard Analysis for Contaminated Sediments Using Stamp Model

Karim Hardy[*], Franck Guarnieri

Center for Research on Risk and Crisis, Mines ParisTech
Rue Claude Daunesse 06904 Sophia-Antipolis Cedex, France
karim.hardy@mines-paristech.fr

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 accident model (Systems-Theoretic Accident Model and Processes) 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 article is organised into three 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). Finally, the third section describes the concrete application of the STPA technique to the Novosol® process.

1. 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 (Depelsenaire, 2006; Breugelmans, 2007) 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 (Novosol®, 2010): 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 (Hardy, 2010).

738

2. The STAMP model and the STPA technique

The STAMP accident model is based on systems control theory. The model was developed by Leveson (2003). In the STAMP model, safety is considered as a problem of control.

2.1 The STAMP model
The STAMP model comprises three interlinked concepts (safety constraints, hierarchical control structures and process models) described below:

- Safety constraints: in contrast to the "classical" view of accidents (that they are due to a series of events), STAMP views accidents as the application of inadequate constraints within the socio-technical system. Safety constraints focus on the relations and decision-making processes that support non-hazardous system states.

- Hierarchical security control structures: in order to prevent, or to analyse accidents, it is necessary to design a hierarchical control structure which represents the socio-technical system in a given context. It must also be capable of representing the constraints described above, both during the development phase, and when the system is fully operational.

- Process models and control loops: a control process (comprising both process models and control loops) operates between each level of the control hierarchy described above. The purpose of the control process is to translate a component, at one level, into a control at another level, either upwards or downwards through the hierarchy. It is represented schematically as a control loop describing the control process.

2.2 The STPA threat analysis 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.

3. Application of the STPA technique to Novosol®

Each of the stages of the STPA methodology are now reviewed and applied to Novosol® (Hardy, 2010):
- Phase 3.1: definition of system requirements with respect to safety and control structures
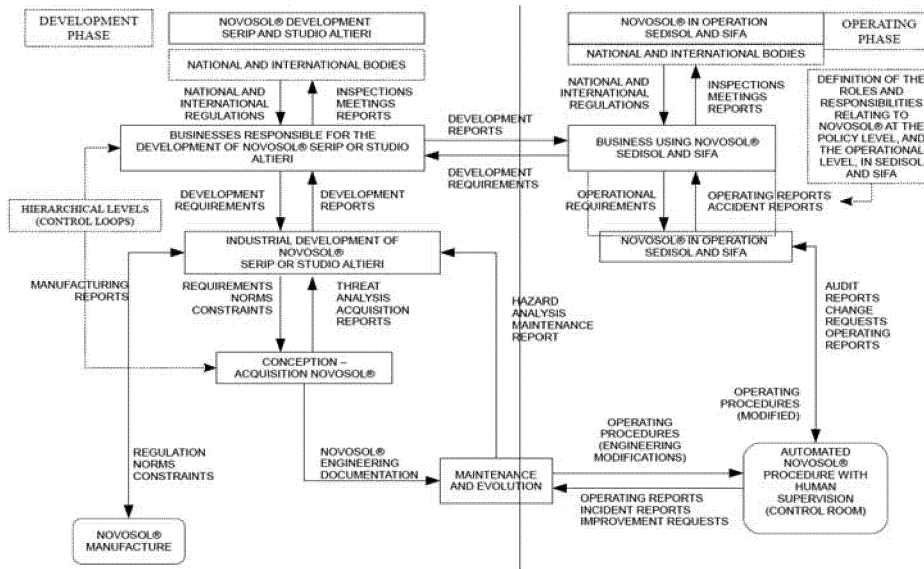

Figure 1: An analysis of Novosol® using the STPA technique. The structure takes into account the development and operation of Novosol®, and shows the interactions between hierarchical levels (Hardy, 2010).

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).

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

The cornerstone of this sub-phase is to define and to establish the control structure for system safety, as described by Leveson (2004). Using the definition of requirements and constraints from the first sub-phase, a hierarchical control structure can be created (Figure 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 supports 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 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).

Table 3: Inadequate control mechanisms 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

- Phase 3.3: Analysis of the process models (control loops (Figure 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.
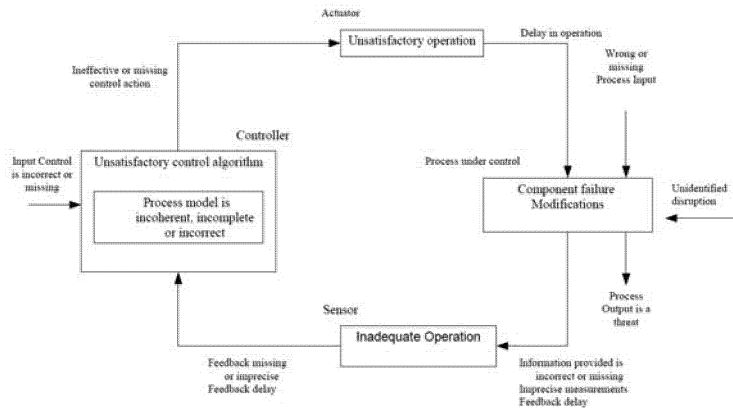

Figure 2: Defects in the control loop. Finding weaknesses in a control loop enables inadequate control actions to be identified.

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, Figure 3 describes the "maintenance and evolution" control loop of the system.
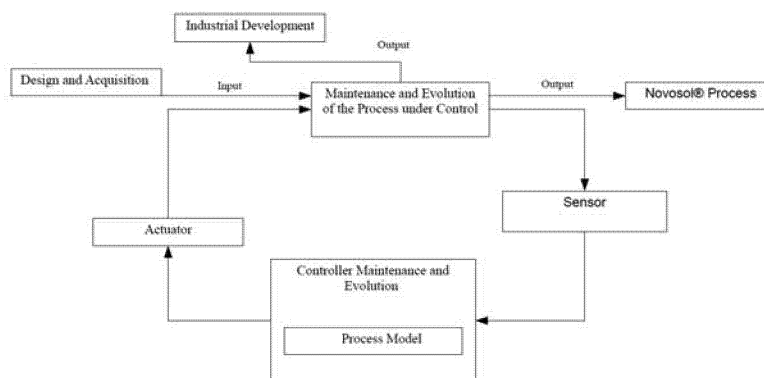

Figure 3: The "maintenance and evolution" control loop of Novosol®. This loop integrates the various components which interact with the process model at a particular level. It highlights interactions at various hierarchical levels.

4. Conclusion

The STPA technique, based on the STAMP model, allows us 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.

Acknowledgements

References

Breugelmans D., 2007, Novosol®: The Story of a Pluridisciplinar Step by Step Approach, Environmental Research and Development, Solvay S.A, Brussels, Belgium.

Depelsenaire G., 2006, Novosol ®: stabilization process for mineral residues contaminated with heavy metals and organic compounds, Solvay S.A, Brussels, Belgium (in French).

Hardy K., 2008, The System Safety Discipline: A Response for Safe Innovative Technologies; A Case Study, International Symposium on Sediment Management, Lille, France.

Hardy K., 2008, Towards a Development of Safe Innovative Systems: Integrating Health and Safety at Work, Conférence Lambda Mu 16, Avignon, France (in French).

Hardy K., 2010, Contribution to the Study of a Model of Systemic Accident, Case of STAMP model: Implementation and Suggestions for Improvement, PhD Thesis, Center for Research on Risk and Crisis, Mines – ParisTech, France (in French).

Leveson N.G., 2003, A New Approach to Hazard Analysis for Complex Systems. International Conference of the System Safety Society. Denver, CO, USA.

Leveson N.G., 2004, A New Accident Model for Engineering Safety Systems. Safety Science 42(4), 237 – 270.

Solvay S.A, 2010, Novosol® <www.novosol.be> accessed 22.02.2011.