



Nordisk kernesikkerhedsforskning
Norrænar kjarnöryggisrannsóknir
Pohjoismainen ydinturvallisuustutkimus
Nordisk kjernesikkerhedsforskning
Nordisk kärnsäkerhetsforskning
Nordic nuclear safety research

NKS-87
ISBN 87-7893-145-2

Barriers, Control and Management Report from the pilot phase

Morten Lind
Technical University of Denmark

September 2003

Abstract

The report documents the results of the pilot phase of the NKS project “Barriers, Control and Management” (NKS-R-07). The following conclusions can be drawn for the work done in the pilot phase:

- A set of research issues and hypotheses to be developed in the main phase of the project has been defined.
- The theoretical work has led to a clarification of the semantic distinctions between safety related actions, control actions and barriers.
- The action concepts of Von Wright have been applied on a case study on the nuclear power plant in Forsmark, Sweden. It has been shown that it is possible to apply the concepts. But it is also concluded that extensions of the theory are required. Such extensions are important objectives for the main phase of the project.

Key words

Formalized concepts, action, function, consistency, procedures, documents

NKS-87
ISBN 87-7893-145-2

Electronic report, September 2003

Published by
NKS Secretariat
P.O. Box 30
DK – 4000 Roskilde, Denmark

Phone +45 4677 4045
Fax +45 4677 4046
www.nks.org
e-mail nks@catscience.dk

Barriers, Control and Management

Report from the pilot phase

Project no NKS-R-07

September 2003

Preface

The present report documents the results of the pilot phase of the NKS project “Barriers, Control and Management” (NKS-R-07). The pilot project was conducted in the period 1/5 until 31/12, 2002 and comprised a total work effort of 5 man months.

Overall Project Goal

The overall goal of the project is to investigate how formalized concepts of action and function can be used to define concepts that can be used in the design and assessment of power plant safety systems and procedures. The aim is to use the generic concepts and give them a concrete interpretation within various safety related contexts of nuclear power plant design and operation. Interpretations from the various contexts are then used to build a minimal set of concepts covering the most important safety activities in nuclear power plants. The usability of the concepts is assessed through applications on e.g. operating procedures, instructions or other types of documents. Application of formalized concepts can increase the consistency of procedures and documents and make them easier to understand and apply by the users in real situations. Furthermore, the supporting set of logically defined action/function concepts facilitates the transfer of procedures and documents to a computer-based system.

The purpose of the pilot phase was to identify and explore the research issues to be addressed in the main project.

Work done and conclusions of the pilot phase

The work done in the pilot phase comprised a combination of analytical work and workshop activities. The purpose of the workshops was to discuss the ideas and problems appearing from the analytical work with other Nordic researchers and industrials.

The analytical activities comprised the following elements:

1. A study has been made of available literature on barrier and defense in depth concepts. Results of this work are included in the present pilot phase report (Lind and Petersen, 2003).
2. At project start it was decided to focus on the modeling of safety work involved in the modification of nuclear power plant components. A contact was established with Olle Andersson at Forsmark Kraftgroup in Sweden who made documents available describing the relevant work procedures and other background information of the plant and the quality assurance system. The safety work involved in the plant modification process was chosen as an empirical case for the modeling work in the pilot phase because it is representative for safety work that involve both organizational and technical safety factors. It was not possible to include other cases in the pilot phase. Analysis of the information acquired from Forsmark has resulted in a preliminary model describing the overall safety management structure (using SADT). The model will be further developed in the main phase of the project.

3. In parallel with the literature review and the empirical modeling activity we have also developed the theoretical basis for the final modeling concepts (Von Wright's action theory). A satisfying logical clarification of the distinctions between prevention (barriers) and control actions has been obtained. These results have been integrated with the empirical modeling work.

The analytical work was combined with workshop activities in a two phased process. Phase one comprised initial analytical work followed by a workshop where the project ideas were introduced to researchers and industrials from the regulators and the nuclear power plant industry. An important function of this workshop was to obtain suggestions, criticism and comments from the industrial participants. Phase two included a compilation of the results of the first workshop and the subsequent development of a model prototype where selected nuclear safety concepts are related to the elementary action types. Project results were also presented and discussed at workshops and technical meeting in the second phase (see table 1).

Table 1. Meetings and workshops

Date	Location	Purpose	Participants
2/5	VTT Automation, Helsinki	Kick Off	Morten Lind Björn Wahlström Carl Rollenhagen Timo Okkonen
23/5	SKI, Stockholm	Presentation of the project for the MTO scientific committee at SKI	Morten Lind Johannes Petersen Björn Wahlström Carl Rollenhagen Representatives from: SKI and Vattenfall Human Factors Scientists from Sweden and Finland
9-10/7	Forsmark 3, Sweden	Acquisition of background information for case	Morten Lind Johannes Petersen Olle Andersson
13 /11	Linköping University	Present and discuss project results	Erik Hollnagel and his research group Martin Fridleifer Morten Lind Johannes Petersen
14/11	SKI, Stockholm	Discuss project issues	Carl Rollenhagen and Olle Andersson Morten Lind Johannes Petersen
13/12	Technical University of Denmark, Kgs. Lyngby	Present and discuss project results	Erik Hollnagel and his research group Johannes Petersen Morten Lind Michael May (Force) Jette Lundtang Paulsen (Risø)

Conclusions

The following conclusions can be drawn for the work done in the pilot phase:

- A set of research issues and hypotheses to be developed in the main phase of the project has been defined (Lind, 2003a)(Lind and Petersen, 2003)
- The theoretical work has led to a clarification of the semantic distinctions between safety related actions, control actions and barriers (Lind, 2003b)
- The action concepts of Von Wright have been applied on a case study on the nuclear power plant in Forsmark, Sweden. (Petersen, 2003a and 2003b). It has been shown that it is possible to apply the concepts. But it is also concluded that extensions of the theory are required. Such extensions are important objectives for the main phase of the project.

References

- Lind, M. (2003a). Research issues and hypotheses. In: NKS project NKS-R-07: Barriers, Control and Management- Report from the pilot phase (this report).
- Lind, M. (2003b). *Promoting and Opposing. A Semantic analysis of Von Wright's action types.* In: NKS project NKS-R-07: Barriers, Control and Management- Report from the pilot phase (this report).
- Lind, M and Petersen, J. (2003). *A review of Barrier Concepts.* In: NKS project NKS-R-07: Barriers, Control and Management- Report from the pilot phase (this report).
- Petersen, J. (2003a). *Analysis of the Plant Modification Process at Forsmark Kraftgroup (AB FKA).* In: NKS project NKS-R-07: Barriers, Control and Management- Report from the pilot phase (this report).
- Petersen, J. (2003b). *Modeling Plant Modification Processes Using Von Wriugh's Action Concepts.* In: NKS project NKS-R-07: Barriers, Control and Management- Report from the pilot phase (this report).

Report structure

The present report is a compilation of working notes produced in the pilot phase of the project. Only a minor editing effort has been done on the original working notes restricted to bringing them into a common format and to establish consistent cross referencing.

Table of Contents

Research issues and hypotheses	5
A Review of Barrier Concepts	12
Promoting and Opposing: A Semantic Analysis of Von Wright's Action Types	18
Analysis of the Plant Modification Process at Forsmark Kraftgroup (AB FKA)	30
Modeling Plant Modification Processes Using Von Wright's Action Concepts.....	38

Research issues and hypotheses

Morten Lind, Ørsted DTU

Introduction

This chapter presents a selection of core issues and research hypotheses that has been identified and elaborated in the pilot phase of the NKS project “Barriers, Control and Management”. The main purpose of the pilot project is to identify and shape the research problems implied by the objectives stated in the original application for the NKS-R-07 project. These research problems will be investigated in the main project.

Objectives of the NKS-R-07 Project

The overall objective of the project is to investigate the use of formalized concepts of action and function to define concepts that can be used in the design and assesment of power plant safety systems and procedures. The aim is to use the generic concepts and give them a concrete interpretation within various safety related contexts of nuclear power plant design and operation. Interpretations from the various contexts are then used to build a minimal set of concepts covering the most important safety activities in nuclear power plants. The usability of the concepts is assessed through applications on e.g. operating procedures and other types of documents. Application of formalized concepts can increase the consistency of procedures and documents and make them easier to understand and apply by the users in real situations. Furthermore, the supporting set of logically defined action/function concepts facilitate the transfer of procedures and documents to a computerbased system.

Core concepts in NPP safety

Safety work in the field of Nuclear Power Plants has evolved from many years of experience in design, regulation and operation of nuclear and conventional power plants and other process industries. The following set of “core” safety concepts has emerged from this activity: *defense in depth, barriers and safety functions*. These concepts are used to formulate safety requirements to the NPP systems and its operations.

Defense in Depth

Defense in depth (DID) is a strategy for design of safe systems (INSAG, 1996). The general idea of DID is to provide several levels of defense against the development of system failures. DID can be seen as a normative design principle derived from the basic anatomy of accidents (Figure 1). The development of an accident is critically dependent on the failure of a series of obstacles or barriers to fault propagation. These barriers include systems or procedures for prevention, control, protection and mitigation of the consequences of events. The barriers comprise in this way a levelled approach to safety management. DID is applied on the physical level to manage the containment of radioactive materials in the NPP, for the design of the protection systems and on an organizational level. The concepts of redundancy, diversity and separation are closely connected with DID and are independent structural and functional principles for design of reliable systems.

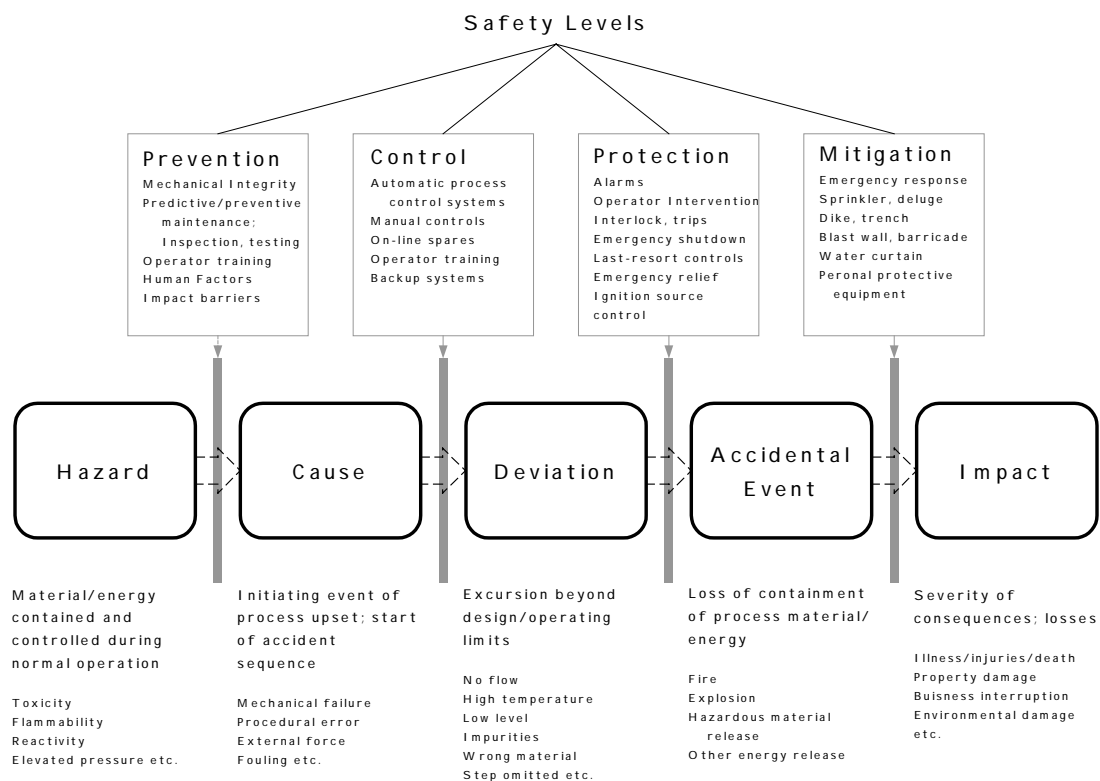


Figure 1. Anatomy of an accident (DOE, 1996)

Barriers

The concept of a barrier is an integral part of the principles of defense in depth. The barrier concept was proposed by Haddon(1973), was later integrated with MORT by Trost and Nertney (1985) in “barrier analysis” and has been further extended by Hollnagel(1999) by several interpretations. Kecklund, Edland and Svenson (1996) use the barrier concept to analyze incidents in nuclear power plants.

It should be noted that the concept of barrier has both a normative and descriptive use. In defense in depth, a barrier is seen as an object of design whereas a barrier in the analysis of incidents refers to any causal factor or process that prevents fault development.

Safety Functions

Safety requirements for nuclear power plants are often specified by the functions that should be provided by plant designers to support various goals or objectives of safety. These so-called safety functions are specified on several levels of decomposition. The following overall safety functions are required (IAEA, 2000)

1. Control of reactivity
2. Removal of heat from the core
3. Confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases.

These overall safety functions can be further decomposed as shown in appendix A into 19 functions. It is seen that specifications of safety functions refer to action concepts (e.g. remove, maintain, prevent, control etc.). Corcoran et. al. (1981) define also safety functions as "a group of *actions* that prevent melting of the reactor or minimize radiation releases to the general public". He identifies four classes of functions:

1. anti-core-melt safety functions
2. containment integrity safety functions
3. control of indirect radioactive releases
4. maintenance of vital auxiliaries needed to support the other safety functions

It is seen that these functions deviate from the functions mentioned above. This disagreement illustrate the difficulty of agreeing on a common level of abstraction in the specification of safety functions. Corcoran relates also safety functions to safety objectives and to so-called success paths (table 1 and 2). He emphasizes in this way the importance of embedding functional specifications into a goal-means framework (Lind, 1994).

Table 1. Nuclear power-plant safety functions (Corcoran et. al., 1981)

Safety function	Safety Objectives
<u><i>Anti-core-melt functions</i></u>	<u><i>Prevent core melt down</i></u>
Control of reactivity	Shut reactor down to reduce heat production
Control of reactor coolant system inventory	Maintain a coolant medium around the core
Control reactor coolant pressure	Maintain the coolant in the proper state
Remove core heat	Transfer heat from the core to a coolant
Reactor coolant system heat removal	Transfer heat from the core coolant
<u><i>Containment integrity functions</i></u>	<u><i>Prevent release of radioactivity</i></u>
Close openings in containment	Isolation of containment
Control of containment temperature and pressure	Avoid damaging containment and equipment
Control of combustible gasses	Prevent explosion inside containment
<u><i>Ensure availability of vital auxiliaries</i></u>	<u><i>Maintain operability of systems needed to support the safety systems</i></u>
Ensure availability of ultimate heat sink	
Ensure availability of electric power supply	Maintain operability of electrically driven equipment
Ensure availability of component cooling water	Keep component operating temperatures within limits
Ensure availability of instrument air supply	Maintain operability of instrumentation systems
<u><i>Control of indirect radioactivity releases</i></u>	Contain miscellaneous stored radioactivity to protect the public and avoid distracting operators from the protection of larger sources of radioactivity.
Fuel pool cooling	
Waste processing	
Spray chemical addition	

Table 2. Success paths corresponding to anti-core-melt safety functions.

Anti-core-melt safety functions	Possible success paths	Associated equipment
Reactivity control	1	Control-element-drive mechanism control system, control element assemblies, motor generator sets, chemical and volume control system (charging and letdown), refuelling water tank.
	2	Reactor protection system, reactor trip switchgear, control element assemblies, chemical and volume control system, boric acid makeup tank
	3	Reactor protection system, reactor trip switchgear, control element assemblies, engineered-safety-features actuation system, safety injection system, refuelling water tank.
	4	Voiding, engineered-safety-features actuation system, safety injection systems, refuelling water tank.
Control of RCS pressure	1	Pressurizer pressure control system, pressurizer spray valves, pressurizer heaters, reactor coolant pumps.
	2	Primary safety valves, auxiliary spray valves, chemical and volume control system, refuelling water tank.

Corcoran group the equipment (physical means) used to realize safety functions into so-called *success paths*. Success paths corresponding to selected anti-core-melt safety functions are shown in table 2.

Research Issues and Hypotheses

The sections below outline a set of tentative research issues and hypotheses, which have been identified in the pilot project. The issues and hypotheses are grouped according to the core safety concepts defense in depth, barriers and safety functions.

Research Issues

Defense in depth and barrier concepts

The generality of the DID principle can be seen both as an advantage and as a problem. It is an advantage because DID provides a generic framework to implement safety in complex socio-technical systems like NPP's. However, the generality is also a problem because systematic assessments of systems safety require finer conceptual distinctions that can cope with the specific characteristics of sub-domains of safety (e.g. containment of radioactive materials and protection systems). As a consequence, there is a danger that safety requirements can turn out to be ambiguous, inconsistent and incomplete.

The following research questions/issues are proposed in order to develop a more formal basis for DID:

1. Understanding the principles of DID require the appreciation of an underlying conceptual schema “explaining” the logic of the levels and their ordering. Can each of the safety levels (prevention, control, protection and mitigation) and their ordering be derived from such a logical basis?
2. It is a problem that each level of safety refers to diverse contexts and meanings of the barrier concept. Can this confusion be resolved by applying the defense in depth principle recursively i.e. can each level of safety (prevention, control,

protection and mitigation) be managed through the same principle and will there to each application be specific interpretations of the barrier concept?

Safety Functions

The concept of safety functions is widely used and accepted but not particularly well defined or formalised. It is therefore difficult to tell whether the safety functions are consistent and to evaluate their completeness. Specification of safety functions is an important part of safety requirements for nuclear power plants and there is therefore a risk that the lack of formalisation could result in reduced levels of safety.

The following research questions/issues are proposed in order to develop a more formal basis for the specification of safety functions:

1. Safety functions are simply functions that support safety objectives. They do not therefore in principle deviate in their logical form from other plant functions supporting e.g. objectives of power production.
2. How are safety functions distinguished from safety objectives and goals?
3. Safety functions specify the means provided to implement the barriers and controls. The concepts of defense in depth and safety functions are therefore related. Can this relationship be expressed through goal-means relations?

Research hypotheses

It is suggested to approach the research issues above by using VonWright's elementary action types (see table 3) and role concepts (agent, object etc.) from e.g. natural language semantics (Petersen, 2000)(Halliday, 1985)(Lyons, 1994) to formalize the semantics of safety levels and safety functions. This hypothesis is supported by the fact that actions of prevention and protection are both instances of the elementary action types *suppress* (or *destroy*) in Von Wrights theory and because prevention and protection actions are distinguishable by different so-called role structures. The concept of barrier will in such a formalization turn out to be a role (participant – role). The

Table 3. Elementary changes, interventions and omissions (Lind, 2000).

Elementary change	Elementary intervention	Elementary omission
$\sim pTp$ p happens	$\sim pT[pI\sim p]$ produce p	$\sim pT[pIp]$ let p happen
pTp p remains	$pT[pI\sim p]$ maintain p	$pT[pIp]$ let p remain
$pT\sim p$ p disappear	$pT[\sim pIp]$ destroy p	$pT[\sim pI\sim p]$ let p disappear
$\sim pT\sim p$ p remains absent	$\sim pT[\sim pIp]$ suppress p	$\sim pT[\sim pI\sim p]$ let p be absent

elementary action types can also formalize control actions because each action type (produce, maintain, destroy and suppress) corresponds to a subtype of control actions

(steering, regulation, tripping and interlock). Insights from Multilevel Flow Modeling (Lind, 1994 and 1999) will also be used to develop formalized concepts to represent goal-means structures for safety.

References

- Corcoran, W. R., Finnicum, D. J., Hubbard, F. R., Musick, C. R. and Walzer, P. F. 1981. *Nuclear Power-Plant Safety Functions*. Nuclear Safety, Vol. 22, No. 2, March-April.
- DOE. 1996. *Chemical Process Hazards Analysis*. DOE –HDBK-1100-96.U.S. Department of Energy, Washington, D.C.
- Haddon, W. Jr. 1973. *Energy Damage and the Ten Countermeasure Strategies*. Human Factors, 15(4), 355-366.
- Halliday, M. A. K. 1994. *An Introduction to Functional Grammar*. Edward Arnold, London.
- Hollnagel, E. 1999. *Accidents and Barriers*. Proc. Seventh. European Conference on Cognitive Science Approaches to Process Control – CSAPC’99. Villeneuve d’Asc France, 21-24 Sept.
- IAEA. 2000. *Safety of Nuclear Power Plants: Design - Requirements*. IAEA Safety Standards Series No. NS-R-1.
- INSAG. 1996. *Defense in Depth in Nuclear Safety*. IAEA, Vienna.
- Kecklund, L. J., Edcland, A., Wedin, P. and Svenson, O. 1996. *Safety barrier function analysis in a process industry: A nuclear power application*. Industrial Journal of Industrial Ergonomics, vol. 17, 275-284.
- Lind, M. 1994. *Modeling Goals and Functions of Complex Industrial Plant*. Applied Artificial Intelligence, Vol. 8, No. 2.
- Lind, M. 1999. *Plant Modeling for Human Supervisory Control*. Transactions of the Institute of Measurement and Control, Vol 21. No 4/5, pp.171-180.
- Lind, M. 2000. *Actions, Functions and Failures in Dynamic Environments*. Centre of Human Machine Interaction. Working Report No. CMHI-8-2000.
- Lyons, J. 1994. *Semantics*. Cambridge University Press.
- Petersen, J. 2000. *Knowledge Based Support for Situation Assessment in Human Supervisory Control*. PhD Thesis from Department of Automation, Technical University of Denmark.

Appendix 1: NPP Safety Functions

The following safety functions is the result of a review of various reactor designs showing that current design requirements can be met by having structures, systems and components that perform the following functions (IAEA, 2000). Note! Can be aggregated into four overall safety functions.

1. to prevent unacceptable reactivity transients
2. to maintain the reactor in a safe shutdown condition after all shutdown actions;
3. to shut down the reactor as necessary to prevent anticipated operational occurrences from leading to design basis accidents and to shut down the reactor to mitigate the consequences of design basis accidents;
4. to maintain sufficient reactor coolant inventory for core cooling in and after accident conditions not involving the failure of the reactor coolant boundary;
5. to maintain sufficient reactor coolant inventory for core cooling in and after all PIEs considered in the design basis;
6. to remove heat from the core¹ after a failure of the reactor coolant pressure boundary in order to limit fuel damage;
7. to remove residual heat (see footnote 1) in appropriate operational states and accident conditions with the reactor coolant pressure boundary intact;
8. to transfer heat from other safety systems to the ultimate heat sink²
9. to ensure necessary services (such as electrical, pneumatic, hydraulic power supplies, lubrication) as support functions for a safety system;
10. to maintain acceptable integrity of the cladding of the fuel in the reactor core;
11. to maintain the integrity of the reactor coolant pressure boundary;
12. to limit the release of radioactive material from the core containment in accident conditions and conditions following an accident;
13. to limit the radiation exposure of the public and site personnel in and following design basis accidents and selected severe accidents that release radioactive materials from sources outside the reactor containment;
14. to limit the discharge or release of radioactive waste and airborne radioactive materials to below prescribed limits in all operational states;
15. to maintain control of environmental conditions within the plant for the operation of safety systems and for habitability for personnel necessary to allow performance of operations important to safety;
16. to maintain control of radioactive releases from irradiated fuel transported or stored outside the reactor coolant system, but within the site, in all operational states;
17. to remove decay heat from irradiated fuel stored outside the reactor coolant system, but within the site;
18. to maintain sufficient subcriticality of fuel stored outside the reactor coolant system but within the site;
19. to prevent the failure or limit the consequences of failure of a structure, system or component whose failure would cause the impairment of a safety function.

¹ This safety function applies to the first step of the heat removal system(s). The remaining step(s) are encompassed in safety function (8).

² This is a support function for other safety systems when they must perform their safety functions.

A Review of Barrier Concepts

Morten Lind and Johannes Petersen, Ørsted DTU

Introduction

The purpose of this chapter is to review selected literature on the barrier concept in the light of the action concepts used in the present project (Lind, 2000a and b). The barrier concept is widely used within safety but there is not much literature discussing the concept in depth. We have selected three articles/reports here for review that we consider of importance for the theoretical development of the concept. The first article is authored by Haddon (1973), who to our knowledge is one of the first trying to develop a theoretical approach to the analysis of safety. The second source is the MORT analysis technique, which is a development based on Haddon's work (Trost and Nertney, 1985). The third author is Hollnagel (1999) who has presented an extension of the domains of application of the barrier concept.

Haddon's strategies

The paper by Haddon (1973) has been quite influential on later safety thinking. Haddon describe in his paper ten general countermeasure strategies for reducing or avoiding energy damages and introduces the barrier concept. In the following we will review the strategies and relate them to the concepts and theories of action used in the current project (Lind, 2000a and 2000b).

The strategies represent, according to Haddon, a generalization across many domains of experiences on countermeasures used to reduce the possibility and consequences of undesirable events. The domains mentioned in the article by Haddon include, among others, various branches of industrial production (nuclear and conventional energy, chemical), the area of transportation, the use of utensils in households, the military, general work safety, hospitals and health care and sports.

We find the ten strategies interesting of two reasons. They represent a generalization over a large field of experience and the strategies have an implicit underlying logic that can be revealed when they are analyzed from an action theoretical perspective. We will indicate the relations to the theory presented in (Lind, 2000a and b) below.

The relations are shown in table 1. The left column in the table contains descriptions of the ten strategies (taken from Haddon, 1973) and the right column indicates our commentary on our interpretation of the strategies. We have reduced Haddon's original description in order highlight the sentences that are relevant for our present purpose.

Table 1. Haddons's ten strategies

Haddon's description	Our interpretation
<p>The <i>first</i> strategy is to prevent the marshalling of the form of energy in the first place: preventing the generation of thermal, kinetic, or electrical energy, or ionizing radiation; the manufacture of gunpowder; the concentration of U-235; the build-up of hurricanes, tornadoes, or tectonic stresses; the accumulation of snow where avalanches are possible; the elevating or skiers; the raising of babies above the floor, as to cribs and chairs from which they may fall; the starting and movement of vehicles; and so on, in the richness and variety of ecologic circumstances.</p>	<p>The first strategy is to prevent the existence of a potential for an undesirable event to happen. Or phrased differently, to prevent that an agent or a system has the power or capability to cause an undesirable event.</p> <p>Haddon's cases exemplify here the <i>prevention of the generation</i> of energy or dangerous substances (U-235) or forces (hurricanes, snow, elevation or moving of objects).</p> <p>The first strategy relate to an agents capability for action. Logically, there can be no action unless the agent has the required capability. An action can therefore be prevented by setting up conditions where the agent cannot acquire the capability to act (Lind, 2000a).</p>
<p>The <i>second</i> strategy is to reduce the amount of energy marshalled: reducing the amounts and concentrations of high school chemistry reagents, the size of bombs or firecrackers, the height of divers above swimming pools, or the speed of vehicles.</p>	<p>Here it is assumed that the conditions for acquiring the capability for action are satisfied. The purpose of the second strategy is then to reduce the capability or power of the agent. The less energy or dangerous substance is accumulated.</p>
<p>The <i>third</i> strategy is to prevent the release of the energy; preventing the discharge of nuclear devices, armed crossbows, gunpowder, or electricity; the descent of skiers; the fall of elevators; the jumping of would-be suicides; the undermining of cliffs; or the escape of tigers.....</p>	<p>The third strategy mark an important transition from countermeasures directed towards the <i>capability</i> for action to countermeasures that inhibit or hinder the <i>realization</i> of the action capability.</p>
<p>The <i>fourth</i> strategy is to modify the rate of spatial distribution of release of the energy from its source: slowing the burning rate of explosives, reducing the slope of ski trails for beginners, and choosing the reentry speed and trajectory of space capsules. The third strategy is the limiting case of such release reduction, but is identified separately because in the real world it commonly involves substantially different circumstances and tactics.</p>	<p>Here it is assumed that the capability for action has been realized. The purpose of the fourth strategy is then to limit the consequences of the action in time and space. As mentioned by Haddon, this may seem as a limiting case of the third strategy but should be kept as a separate category. We agree because there is a distinct difference between hindering the realization of an action (third) and to reduce or abstain from exercising the capability for the same action (fourth).</p>
<p>The <i>fifth</i> strategy is to separate, in space or time, the energy being released from the susceptible structure, whether living or inanimate; the evacuation of the Bikini islanders and test personnel, the use of sidewalks and the phasing of pedestrian and vehicular traffic, the elimination of vehicles and their pathways from community areas commonly used by children and adults, the use of lightning rods, and the placing of electric power lines out of reach.....</p>	<p>The fifth strategy marks another important transition this time shifting the focus from the agents capability for action (strategies 1-5) to considering the opportunities for action. The strategy eliminates the opportunities by separating the agent and the objects of interest in space and time. Since the agent and the object do not occupy the same space-time location there is no opportunity for action.</p>
<p>The very important <i>sixth</i> strategy does not use separation in time and space, but instead uses separation by interposition of a material "barrier"; the use of electrical and thermal insulation, shoes, safety</p>	<p>In the sixth strategy, the action of the agent is counteracted by interposing a material object that is able to eliminate the effects of the agents action on the environment. Such a material</p>

glasses, shin guards, helmets, shields, armor plate, torpedo nets, antiballistic missiles, lead aprons, buzz-saw guards, and boxing gloves.	object serves as a <i>barrier</i> against the agents actions. In other words, the barrier is a functional concept describing how an object is used in a given context.
The <i>seventh</i> strategy, into which the sixth blends, is also very important. This strategy appropriately modifies the contact surface, subsurface, or basic structure, as in eliminating, rounding and softening corners, edges, and points with which people can, and therefore sooner or later do, come in contact.	As noted by Haddon this is a variant of the sixth strategy- Instead of eliminating completely the effects the agents action, the effects is reduced.
The <i>eighth</i> strategy in reducing losses in people and property is to strengthen the structure, living or nonliving that might otherwise be damaged by the energy transfer. Common tactics, often expensively under-applied, include tougher codes for earthquake, fire, and hurricane resistance, and for ship and motor vehicle impact resistance. The training of athletes and soldiers has a similar purpose, among others, as does the treatment of hemophiliacs to reduce the results of subsequent mechanical insults. A successful therapeutic approach to reduce the osteoporosis of many post-meno-pausal women would also illustrate this strategy, as would a drug to increase resistance to ionizing radiation in civilian or military experience. (Vaccines, such as those for polio, yellow fever, and smallpox, are analogous strategies in the closely parallel set to reduce losses from infectious agents.)	The eight strategy should be compared with the strategies mentioned above which all aim to hinder or reduce the agents capability for action and to reduce the effects on the environment. The eight strategy represents countermeasures that make the environment or the object of action immune or insensitive to impacts. The focus is here on protecting the object rather than preventing intervention by the agent.
The <i>ninth</i> strategy in loss reduction applies to the damage not prevented by measures under the eight preceding. This strategy is to move rapidly in detection and evaluation of damage that has occurred or is occurring, and to counter its continuation extension. Elements in this include; the generation of a signal that response is required; the signal's transfer, receipt, and evaluation; and the decision and, follow-through.	The ninth strategy marks yet another shift from considering various measures that oppose the interaction between the agent and the environment to the introduction of another agent that monitor and evaluate the interaction and make decisions.
The <i>tenth</i> strategy encompasses all the measures between the emergency period following the damaging energy exchange and the final stabilization of the process after appropriate intermediate and long-term reparative and rehabilitative measures. These may involve return to the pre-event status or stabilization in structurally- or functionally-altered states.	The tenth strategy represent the compensatory control actions performed by the monitoring agent in response to a decision to intervene.

Summary on Haddon's strategies

It is seen that Haddon's strategies cover a very wide spectrum of safety related situations. The strategies represent a systematic shift of attention or focus on the interaction between an agent and an environment. However, the ninth and the tenth strategies relate to control issues and do therefore belong to a separate category incompatible with the first eight strategies. It should be noted that Haddon only use the concept of barriers in connection with material objects. The later developments in MORT and by Hollnagel generalize the barrier concept to cover the other strategies as well. We think that this is a source of semantic problems because the implicit distinctions in agent-object relationships that are revealed above in our analysis of Haddon's strategies are lost in the generalization.

MORT

According to the MORT (The Management Oversight and Risk Tree) system safety programme the basic ingredients of an accident are (Troost and Nertney, 1985):

- the energy flow or environmental condition that does the harm;
- the vulnerable people or objects that can be hurt by that energy flow or environmental condition;
- the failure or lack of the barriers and controls that are designed to keep them apart; and
- the events and energy flows that lead into the final accident phase.

Like Haddon (1973) the MORT programme uses an energy-barrier concept. A distinction is made between *safety* and *control barriers*. Safety barriers is concerned with control of unwanted energy flows and control barriers are concerned with the control of wanted energy flows. A barrier can be both a control barrier and a safety barrier.

Examples of safety barriers are: protective equipment, guardrails, safety training, work permit, and emergency plans. Examples of control barriers are: conductors, approved work methods, job training, disconnect switch, and pressure vessels.

Note that, compared to Haddon (1973) the MORT programme generalizes the barrier concept. Haddon uses of the barrier concept only as a material separation of harmful energy and the target.

The analytical description of barriers in the MORT programme is based on concepts such as *function*, *location* and *type*. The function of a barrier can be prevention, control or minimization. A barrier can be located on the energy source, between the source and the worker, on worker, and separation through time and space. The different types of barriers are physical barriers, equipment barriers, warning devices, procedures/work processes, knowledge and skill, and supervision.

Furthermore, a strategy for dealing with hazards is described. The priority of actions is:

1. Elimination through design selection.
2. Installation of safety devices (barriers).
3. Installation of warning devices for timely detection (barriers).
4. Development of special procedures enabling the equipment operator to handle the situation (barriers).

The limitation of barriers is discussed. A barrier can be impractical (either not possible or not economic), it can fail (either partially or totally), and it may not be used (either not provided or not used due to worker error).

Hollnagel's extensions of the barrier concept

Hollnagel (1999) defines a barrier as an obstacle, an obstruction or a hindrance that may 1) prevent an action from being carried out or an event from taking place, or 2) prevent

or lessen the impact of the consequences. Note that this definition marks a generalization of the concept of a barrier as it is not restricted to an energy-based concept.

A *barrier function* can be defined as the specific manner by which the barrier achieves its purpose, whereas a *barrier system* can be defined as the substratum or foundation for the barrier function, i.e. the organizational and/or physical structure without which the barrier could not be accomplished.

According to Hollnagel(1999) an analytical description of barriers can be based on different concepts, such as the barrier's *origin*, their *purpose*, their *location*, and their *nature*. Hollnagel argues that only the concept of the barrier nature is rich enough to support an extensive classification of barrier systems. He makes a distinction between material, functional, symbolic and immaterial barriers.

Material barriers:

Barriers that physically prevent an action from being carried out or the consequences from spreading. Examples of material barriers are buildings, walls, fences and railings.

Functional (or active or dynamic) barriers:

Barriers that work by impeding the action to be carried out, for instance by establishing a logical or temporal interlock. A functional barrier effectively sets up one or more preconditions that have to be met before something can happen. Examples of functional barriers are: a lock (physical or logical)

Symbolic barriers:

Barriers that require an act of interpretation in order to achieve its purpose. Hence, such barriers presume an "intelligent" agent that can react or respond to the barrier.

Immaterial barriers:

Barriers that are not physically present in the situation but depend on the knowledge of the user to achieve their purpose. Immaterial barriers are usually also present in a physical form such as a book or a memorandum, but physically present when the use is mandated.

Summary on Hollnagel's extensions

It seems that Hollnagel's treatment of the barrier concept is predominantly human-centered. Only the material and the functional barriers are relevant in relation to the prevention of an action of a physical system or the prevention of the happening of the consequences of such an action. Hollnagel's categories of barrier systems covers the different barrier types mentioned in the MORT programme.

References

- Haddon, W. (1973). *Energy Damage and the Ten Countermeasure Strategies*. Human Factors, 15(4), 355-366.
- Hollnagel, E. (1999). *Accidents and Barriers*. Proc. Cognitive Science Approach to Process Control.

Lind, M. (2000a). *Possibilities for Action*. Report from Center of Human Machine Interaction CHMI-7-2000.

Lind, M. (2000b). *Action, Functions and Failures in Dynamic Environments*. Report from Center of Human Machine Interaction CHMI-8-2000.

Trost, W. A. and Nertney, R. J. (1985). Barrier Analysis. EG&G Idaho Falls, Rept. No. SSDC-29.

Promoting and Opposing: A Semantic Analysis of Von Wright's Action Types

Morten Lind, Ørsted DTU

Introduction

The purpose of the present study is to solve a set of semantic problems that appear when the action types of Von Wright(1963) are used in the modeling of complex human-machine systems (Lind, 2000). The following related problems have been investigated:

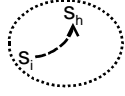
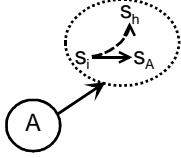
- There is an ambiguity in the use of the action types. When an agent interacts with the environment, the result of the action can be seen both as a promotion and as a prevention of a state of affairs. This ambiguity appears in the analysis of safety related systems where it is often difficult to decide whether a system should be assigned a barrier function (prevention) or a control function (promotion). We will show that this ambiguity can be resolved by distinguishing between the overt (observable) and the covert (intentional) aspects of an action. The overt aspects of an action are represented in an *action schema* that can be given different interpretations taking into account the covert aspects of the action. The interpretations are represented in *action descriptions*.
- Another related issue is the problem of event interpretation in safety analyses like MTO analysis (Rollenhagen, 1997). Here it is a problem to reveal the underlying causes for incidents or accidents such as barrier failure. Many interpretations are here possible if the analyst is not well informed about the context. We will show that Von Wright's action types with the extensions mentioned above may be used to generate systematically explanations for an event. The set of explanations generated are dependent on and can be considered complete within a given context of analysis.

The work presented here build on and extends previous work by the present author on Von Wright's action theory (Lind, 2000). In the process of theory development it has also been necessary to revise some of the previous results. Especially the failure types presented in (Lind, 2000) have proven to be partly incorrect. In order to remedy for these flaws and to clarify important but implicit assumptions in Von Wright's theory, the present report contains a slightly revised and extended introduction to Von Wright's theory of elementary action types.

Von Wright's Theory of Action

The purpose of Von Wright's theory of action is to provide a logical definition of the concept of action that could be used to solve problems in the logic of legal arguments. One of the key points in his theory is to define actions so that they can be distinguished logically from other events that happen without the intervention of an intentional agent. This issue is obviously relevant for determining the conditions under which an agent is responsible for his actions. However, the distinction between intentional action and happenings is also important in the analysis of human interaction with complex systems and in understanding the purposes of technical artifacts.

Table 1. Von Wright define actions by two situations

Situation	Explanation	Illustration
Hypothetical with no agent	The state of the environment changes from s_i to s_h by its own dynamics. s_i :the initial state of affairs s_h :the (hypothetical) end-state of affairs had there been no agent	
Actualized with one agent (A)	The agent A intervene and the state of affairs in the environment changes from s_i to s_a instead of s_h	

The Action Concept

Von Wright’s theory considers the interaction between an agent and a dynamic environment and defines an action in terms of state of affairs in the environment in two different situations (table 1). The first situation is hypothetical and describes what would happen in the environment if there were no agent. The second situation is the actual one where the agent interacts with the environment. The action of the agent can then be defined by the difference between the change of state of affairs in a hypothetical situation and the change realized in the actual situation. Since the first situation is hypothetical, an action is accordingly defined on the basis of a counterfactual conditional. It should be noted that an action is defined only with reference to state of affairs, which are observable in principle through a suitable experimental setup. Von Wright formalizes this definition of the action concept by the introduction of two operators T (then) and I (instead).

The T operator represents the change from state of affairs s_i to s_a by the formula $s_i T s_a$ that we will call a *change schema* in the following. The reading of the schema is “initially the state of affairs was s_i then (T) s_a occurred” or more briefly “ s_i then s_a ” .

The operator I describes the relation between the actualized s_a and the hypothetical state of affairs s_h by the formula $s_a I s_h$. Von Wright expresses the logic structure of an action by combining the two operators T and I into the formula $s_i T [s_a I s_h]$, which we will call an *action schema*. The reading of the schema goes as follows: Initially the state of affairs was s_i then (T) s_a occurred instead (I) of s_h . It should be noted that the notion of change implies a notion of time because the operator T means that s_i precedes s_a in time.

Overt and covert aspects

Von Wright’s definition (and thereby the action schema) refers only to the overt aspects of an action. There are no references to covert aspects like the aims or motives of the agent. It is therefore impossible to distinguish between intentional and non- intentional actions. As this distinction is important in the analysis of human machine interaction we will extend the theory in the following to include the intentions of the agent. Such an extension contributes to a solution of the problems of semantic ambiguity mentioned in

the introduction and is also necessary in order to be able to characterize erroneous actions. Before we discuss the extensions we need to introduce Von Wright's elementary types of change and action.

Change Types and Action Types

The starting point of Von Wrights analysis is accordingly that actions of an agent can be characterized by the resulting changes in the environment. Action types can therefore be defined if it is possible to define change types. If we consider the action schema introduced above it is realized that it can be used to generate an infinite number of action *tokens* by proper combination of different state of affairs. There are no restrictions put on s_i , s_a and s_h . But it is obviously interesting to define a small set of *elementary* and *generic* action types. The action types should be elementary because they should be used as “building blocks” to construct more complex action types. And they should be generic in order to allow multiple interpretations. Von Wright has proposed a set of elementary changes and a corresponding set of elementary action types that we will consider in the following.

Elementary Changes

Considering a state of affairs described by the proposition p , Von Wright distinguishes between four types of elementary change as shown in table 2. Here $\sim p$ means that p is not true and the change schema $\sim pTp$ should read ‘ $\sim p$ then p ’.

The four types of change in table 2 are the logically possible combinations. Note that the state of affairs p is generic and may have a variety of interpretations depending on the nature of the environment. In other words the meaning of p depends on how the state of affairs are defined in the domain and problem under investigation. The types of elementary action types derived from the elementary changes can therefore be used to describe situations where multiple representations are necessary in order to describe the interactions between the agent and the environment.

Note also that two items, a schema and a description define each type of change. The schema defines the logical structure of a change whereas the descriptions specify the meaning of the schema. Von Wright does not discuss the distinction between the

Table 2. The elementary change types

Change schema	Description
$\sim pTp$	p happens
pTp	p remains
$pT\sim p$	p disappear
$\sim pT\sim p$	p remains absent

schema and the corresponding description. We will show later that the distinction is important for resolving semantic problems that occur when the theory is used to model the interaction between the agent and the environment.

Elementary Actions

The four elementary change types shown above correspond to eight elementary action types. The eight types can, as shown below, be further divided into four elementary interventions and four elementary omissions if a distinction is made between accidental happenings and intentional actions. By an intervention we mean an action that results in the change of state of affairs in the environment. But in order to distinguish an intervention from a purely accidental happening, we must also assume that the agent intervene with an intention. An omission is defined as an action where the agent decides not to intervene i.e. deliberately let the state of affairs in the environment change by its own dynamics. As stressed by Von Wright, we must assume that the agent both has an opportunity to act and is able to intervene in order to talk meaningfully about an omission. We must also assume that things would have been different had the agent intervened rather than omitted to act.

Elementary interventions

The elementary interventions are obtained from the elementary changes in table 1 simply by extending the change schema with the hypothetical state of affairs that would obtain if the agent did not intervene. Since the intervention should change the environment it is necessary that the state of affairs realized by the action is different from the hypothetical state that would obtain if the intervention were not done. We therefore get the resulting four interventions shown in table 3, each corresponding to an elementary change type. As with changes, each intervention is characterized by a schema and a description. The description conveys the meaning of the action schema. The descriptions in table 3 correspond to the descriptions proposed by Von Wright with a single exception. We use the term 'maintain' instead of the term 'preserve' used by Von Wright.

Table 3. The elementary interventions

Change	Intervention	
	Action Schema	Description
$\sim pTp$ (p happens)	$\sim pT[pI\sim p]$	produce p
pTp (p remains)	$pT[pI\sim p]$	maintain p
$pT\sim p$ (p disappear)	$pT[\sim pIp]$	destroy p
$\sim pT\sim p$ (p remains absent)	$\sim pT[\sim pIp]$	suppress p

We will show later that the same action schema can be given different descriptions depending on covert aspects of the action, which are not included in Von Wright's theory. The descriptions given in table 4 are therefore only temporary.

Elementary Omissions

The elementary omissions are also obtained from the elementary changes by extending the change schema. In the case of omissions, the actualized state of affairs must be the same as the hypothetical state of affairs that would obtain if the agent did not intervene (which he does not). We therefore get the resulting four omissions shown in table 4 each corresponding to an elementary change type. As with the interventions, we have characterized each omission both by its action schema and its description.

Examples

The four types of intervention can be illustrated by assuming that p represents the proposition 'the valve is open.' We will first consider $\sim pT[pI\sim p]$ representing the action of changing a world where $\sim p$ is true into a world where p is true. Thus $\sim pT[pI\sim p]$ whose description is 'produce p ' is in our example represented by the sentence 'the valve is being opened.' The schema $pT[\sim pIp]$ represents the action 'destroy p ' and describes the action of closing the valve. The action schema $pT[pI\sim p]$ represents an intervention that does not change the environment in the feature described by p on two successive occasions. In our example the action schema $pT[pI\sim p]$ would therefore represent the action 'keeping the valve open.' Finally the schema $\sim pT[\sim pIp]$ represents an action that keep the environment unchanged in the feature described by $\sim p$. This action therefore represent 'the suppression of p ' i.e. a situation where the valve is closed but will open unless an agent does not keep it closed.

We can also use the example to illustrate the four types of omission. Thus $\sim pT[pIp]$ whose description is 'let p happen' will correspond to the sentence 'the valve is left open.' The schema $pT[\sim pI\sim p]$ represents the action 'let p disappear' that will be represented by the sentence 'the valve is left closed'. The schema $pT[pIp]$ represents an omission with the description 'let p remain'. The schema $pT[pIp]$ would therefore

Table 4. The elementary omissions

Change	Omissions	
	Action Schema	Description
$\sim pTp$ (p happens)	$\sim pT[pIp]$	let p happen
pTp (p remains)	$pT[pIp]$	let p remain
$pT\sim p$ (p disappear)	$pT[\sim pI\sim p]$	let p disappear
$\sim pT\sim p$ (p remains absent)	$\sim pT[\sim pI\sim p]$	let p remain absent

represent the omission 'letting the valve stay open.' Finally the schema $\sim pT[\sim pI\sim p]$ with the description 'the suppression of p' represents an omission where the agent 'let the valve remain closed'.

Elementary Control Actions

The four elementary interventions correspond to four different types of control actions that are known from control systems engineering. The correspondences are shown in table 5 and it is seen that there is an intervention type for each control action. The action theory provides in this way a theoretical explanation for both the necessity and the sufficiency of the four types of control actions. But the correspondences between control actions and interventions do not provide a complete characterization of control actions. It is also necessary to include the presence of a second counteracting but defeated agent (the actions of this second agent are called disturbances in usual control theoretical terminology). Furthermore, it is also necessary to include acts of observation, decision and intervention i.e. the means of control. Adding types corresponding to omissions may also extend the set of control actions. A more complete representation of control actions would accordingly include several agents and several levels of means-end abstraction. Various aspects of control actions are discussed in (Lind, 2000) and will not be investigated further here.

Action Descriptions

Von Wright does not discuss the distinction between the action schema and the action description. Furthermore, an action schema is always associated with the same description. We will show in the following that this leads to semantic problems that can be resolved by applying multiple descriptions to the same schema. The descriptions are distinguished by referring to the intentions of the agent. The semantic problems can be illustrated by discussing the consequences of reducing the eight action types to four by substituting p with $\sim p$ in the action schemas. The reduced, but semantically problematic set obtained in this way is shown in table 6.

The reduction is possible in principle due to the logical form of the action schemas. To see how the reduced set is derived from the full set of eight elementary actions let us consider the action with description "produce p" and schema $\sim pT[pI\sim p]$.

Table 5. Elementary interventions and corresponding control actions.

Elementary intervention	Control action
Produce	Steer
Maintain	Regulate
Destroy	Trip
Suppress	Interlock

Table 6. Reduced but problematic set of interventions and omissions

Change	Intervention	Omission
$\sim pTp$ p happens	$\sim pT[pI\sim p]$ produce p	$\sim pT[pIp]$ let p happen
pTp p remains	$pT[pI\sim p]$ maintain p	$pT[pIp]$ let p remain

If we substitute p with $\sim p$ we get the description “produce $\sim p$ ” and the schema $\sim(\sim p)T[(\sim p)I\sim(\sim p)]$, which is logically equivalent to the schema $pT[\sim pIp]$, which have the description “destroy p ”. In this way we can derive two descriptions for each action schema as shown in table 7.

It is seen that the logical equivalences in this way can be used to reduce the set of elementary actions to e.g. the four shown in table 6 (other sets are possible). It would now be tempting also to conclude that the two descriptions for each action schema are semantically equivalent. But this is not the case as explained in the following. Interventions and omissions will be considered separately because they require different explanations.

Descriptions of Interventions

The two descriptions for each elementary intervention type are not semantically equivalent because they have different referents. This can be seen by considering e.g. the action description ‘maintain $\sim p$ ’ that refer to the state of affairs ($\sim p$) resulting from the intervention whereas the description ‘suppress p ’ refer to the hypothetical state of affairs (p) that would have obtained if the agent did not intervene. The two descriptions have therefore different meanings.

Table 7. Action schemas and corresponding descriptions

Description 1	Schema	Description 2
produce $\sim p$	$pT[\sim pIp]$	destroy p
maintain $\sim p$	$\sim pT[\sim pIp]$	suppress p
destroy $\sim p$	$\sim pT[pI\sim p]$	produce p
suppress $\sim p$	$pT[pI\sim p]$	maintain p
let $\sim p$ happen	$pT[\sim pI\sim p]$	let p disappear
let $\sim p$ remain	$\sim pT[\sim pI\sim p]$	let p remain absent
let $\sim p$ disappear	$\sim pT[pIp]$	let p happen
let $\sim p$ remain absent	$pT[pIp]$	let p remain

The distinction between two different descriptions of the same intervention is important when explaining events or changes that are results of an agent’s action. But the reductions create problems if we want to describe the same action from both an opposite and

a preventive perspective. They force us to use only one. Consider for example a situation where an agent is ‘maintaining p ’. The same situation could equally well be described as if the agent was ‘suppressing $\sim p$ ’. The two descriptions are logically equivalent and we could be tempted to use one of the equivalent forms for reasons of simplicity and compactness of the theory. However, the possibility to describe the action from two perspectives would then be lost. When the action is described as ‘maintaining p ’ we focus on the result of the action (p) whereas when we describe it as ‘suppressing $\sim p$ ’ we focus on what had happened if the agent did not act ($\sim p$ would happen) i.e. we describe it in relation to a hypothetical state of affairs which is prevented by the action of the agent and not in relation to a state of affairs which is produced. The problem with the reduction is that the two logically equivalent descriptions have different semantics because they refer to two different descriptive situations. We need to be able to express such semantic differences and therefore to abstain from the reduction.

The relations between change types, action schema and action descriptions are shown in figure 1. The action descriptions are grouped horizontally into two types of description distinguished by two complementary action verbs promoting and opposing. According to the first type of description the action is a promotion of state of affairs (e.g. ‘produce p ’) whereas the action is opposive according to the other type of description (e.g. ‘destroy $\sim p$ ’). We can accordingly conclude that the same intervention can be described in two ways either as promoting or opposing state of affairs. This result explains why control actions (promotive) sometimes also are described as opposive actions. A typical example of this apparent ambiguity is when the actions of a driver described as ‘keeping the car running on the road’ also are described as ‘preventing the

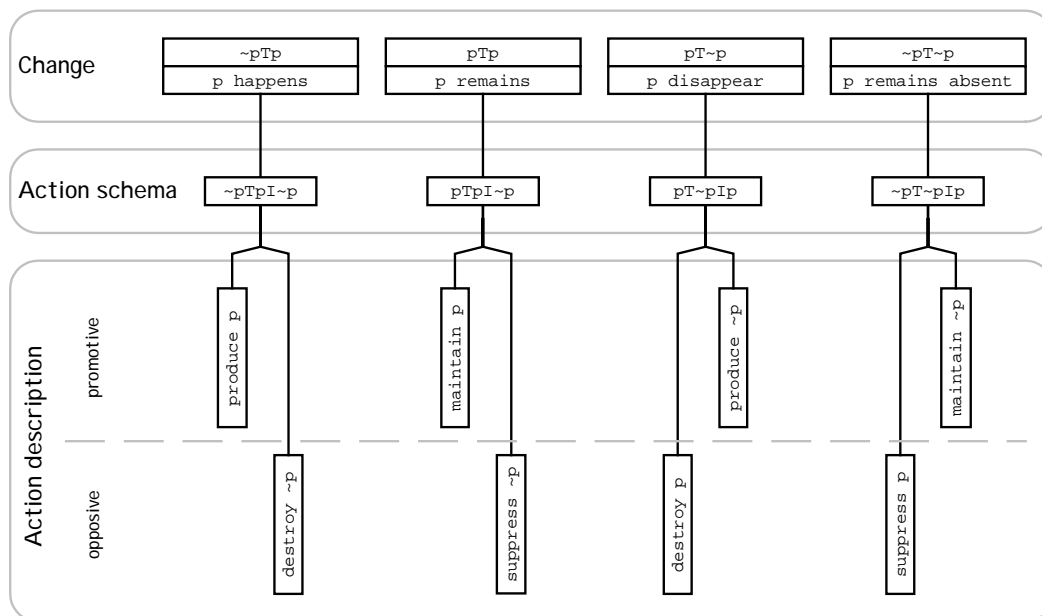


Figure 1. Change and action schemas and descriptions for interventions

car from driving off the road’. The two descriptions refer to the same *observable* behavior represented by the schema, but the question is which of the descriptions should be taken as the proper one? This question is addressed below where it is shown that the

answer depends on motives or intentions of the agent i.e. on covert aspects of the action, which are not included in Von Wright's theory.

Intentions and Descriptions of Interventions

We can use the possibility of dual descriptions to let the description of an action express the motives or intentions of the agent. This can be realized by noting that descriptions of intervention in the 'promotive' mode refer to the state of affairs realized by the intervention. In contrast, descriptions in the 'opposive' mode refer to the state of affairs that would occur if the agent did not intervene. Take as an example the action $pT[pI\sim p]$ which have the alternative descriptions 'maintain p' or 'suppress $\sim p$ '. In the first description we focus on what is promoted (p) whereas we in the latter description focus on what is opposed ($\sim p$). As shown below, the choice of description depends on whether the motive relates to a future (desirable) result of the intervention or if it relates to a (non-desirable) hypothetical state of affairs that is opposed by the agent.

Sometimes the two descriptions of an intervention can be applied at the same time as for example when the agents motive is to 'produce p' and at the same time realizes 'destroy $\sim p$ '. It should be noted that 'producing p' in such cases cannot be seen as a means of 'destroying $\sim p$ ' since the two descriptions are different interpretations of the same event. There is no causal relation involved as there should be in a means-end relationship. There are other situations where it also may be relevant to apply both descriptions such as when the agent has dual motives.

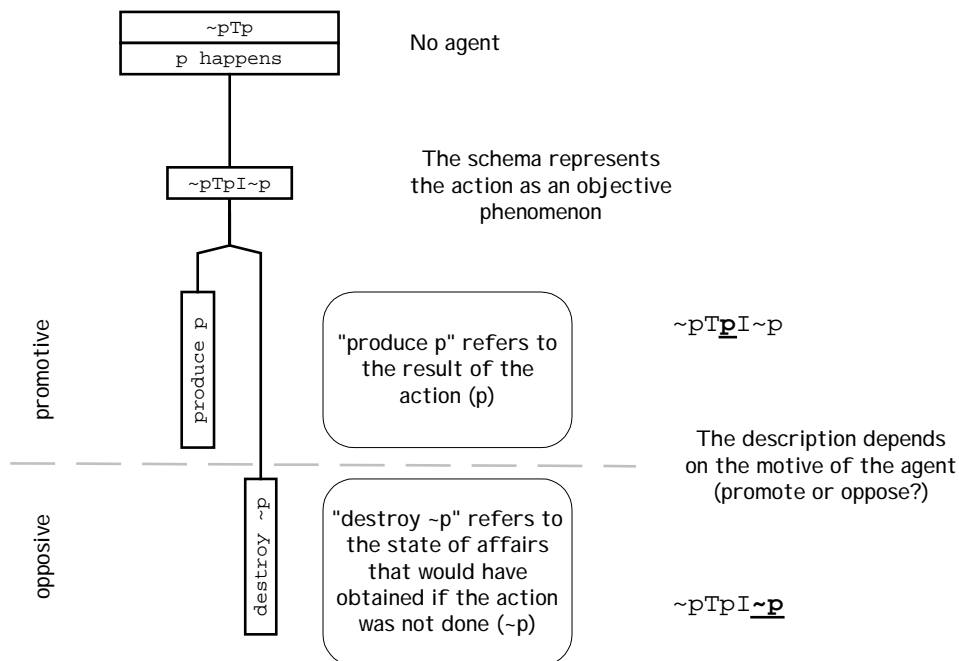


Figure 2. Descriptions of an intervention depends on the motive of the agent

Note that aims or motives could be of different sorts and we have only discussed one of the possibilities. The motive could simply be to intervene in the environment without concern about the specific change of state of affairs in the environment. The aim could also be to obtain a certain result i.e. a desirable state-of-affairs. This is the situation discussed above. However, the aim could also be to bring about a state of affairs that is

a consequence of the result. The intervention could also be part of a plan of action so that the aim would be to produce a condition necessary for the execution of further actions. It is clear that depending on the nature of the motivation we can produce many different descriptions of the action.

The Significance of Initial State of Affairs

The distinctions between the opposite and promotive mode of description related to different motives of the agent. Taking either the promotive or opposite interventions we could also ask how the individual elementary intervention types within the category are distinguished (i.e. produce versus maintain or destroy versus suppress). By analyzing the corresponding action schemas it is realized that they are distinguished only by the initial state of affairs. But it is also realized that they have the resulting state of affairs in common, the reason why they are considered in the same category (promotive or opposite).

Further Remarks on Oppose Actions

It can be seen from the analysis above that actions opposing state of affairs p are subdivided into actions that suppress and destroy. This distinction is, as mentioned above, based on a difference in the initial state of affairs. We will also mention briefly here that interventions that suppress state of affairs can be subdivided further into preventive and protective actions. We have therefore a tree of oppose actions shown in figure 3.

This sub-typing of the suppress action presupposes that the agent is interacting via the environment with another agent. Consider an agent A that intervene the environment with the motive of suppressing state of affairs p , which would otherwise be produced by another agent B. If agent A succeeds we would say that A prevented B from producing p . A preventive act is accordingly described from the perspective of the agents. If the same action were described from the perspective of the environment we would say that that A protects the environment against B's attempt to produce p .

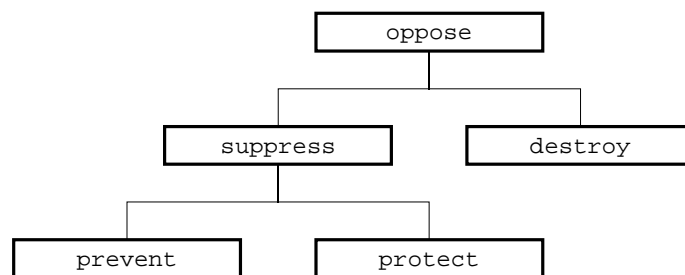


Figure 3. Type tree of oppose actions

Further expansion of the presented work and the theory of two agent situations presented in (Lind, 2000) is required in order to account in detail for the semantics of safety related actions. Barriers are related to both protective and preventive actions and a resolution of the semantic problems with this concept is therefore expected also to be part of this expansion. The expansions are the subject of further work.

Descriptions and Omissions

We can also introduce a distinction between the schema and the descriptions of omissions. Descriptions of interventions were distinguished by the motives of the agent but we cannot refer to motives in the case of omissions. The motives defined the reasons the agent had for intervening in the environment. When the agent omits to act intentionally and let the dynamics of the environment change state of affairs the decision of the agent is motivated by his expectations regarding the behavior of the environment. In circumstances where the agent expect the environment to change by its own dynamics into a desirable state of affairs the agent have no reason to intervene. The dependence of the description on the expectations of the agent is shown in figure 4. The resulting relations between change schemas, action schemas and descriptions for omissions shown in figure 5.

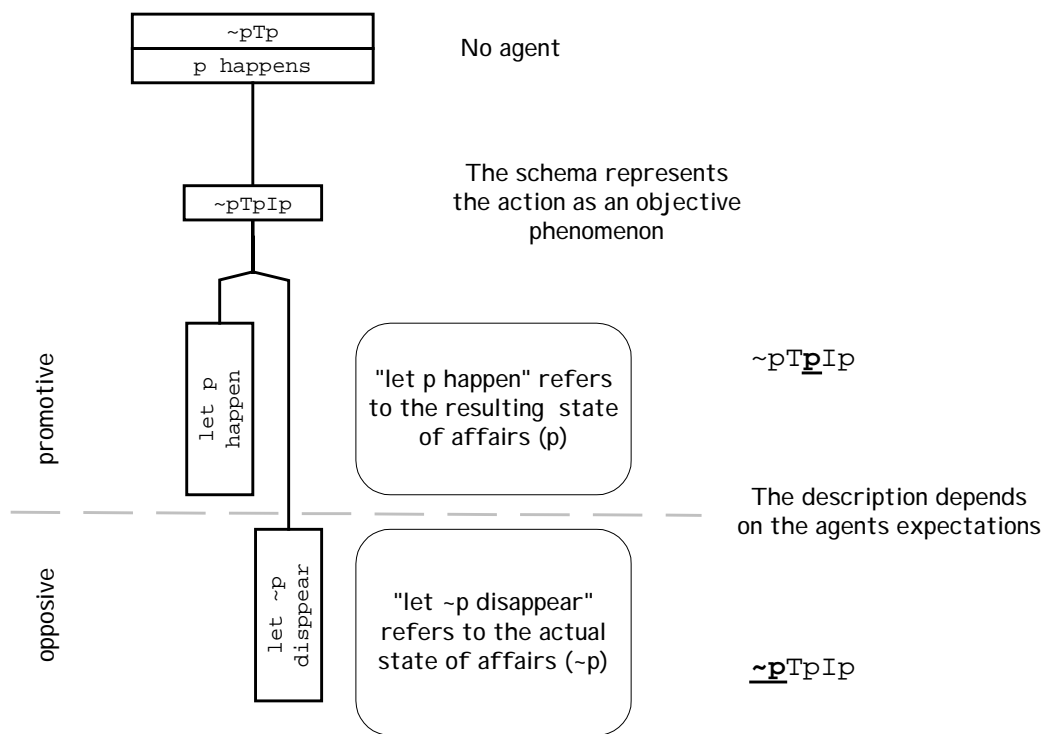


Figure 4. The description of an omission depends on the expectations of the agent

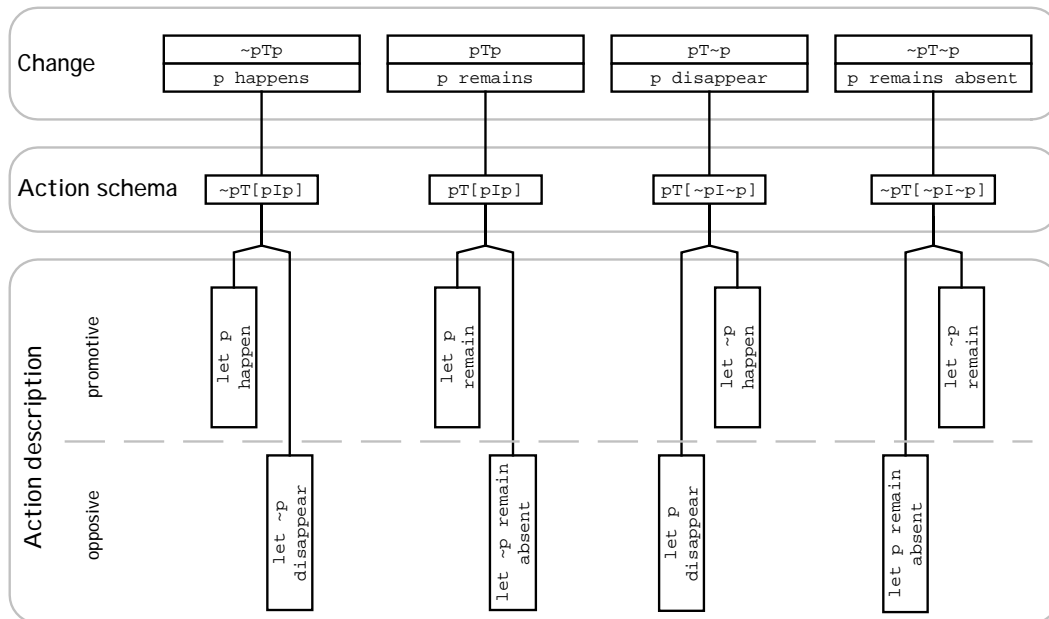


Figure 5. Change and action schemas and descriptions for omissions

Event Interpretation

The analysis of the relations between the change schema, the action schema and action descriptions presented above may also be used to discuss the problem of event interpretation. An event or change can be given many descriptions depending on the context. A change of state of affairs can be described simply as the result of the inherent dynamics in the environment. In such a case we would represent the change simply by its schema. The change could also be seen as the result of an agent's intervention in the environment and we would then represent the change by a corresponding action schema.

Finally we could also represent the change by one of the action descriptions that correspond to the action schema. Here the description of the change will be related to the motives of the agent.

The problem in event analysis is to decide which of the descriptions that should be used in a given situation. This decision cannot be made without making assumptions about the circumstances under which the change of affairs are occurring. These assumptions can be derived from the analysis presented above.

References

- Lind, M. (2000). *Action, Functions and Failures in Dynamic Environments*. Report from Center of Human Machine Interaction CHMI-8-2000.
- Rollenhagen, C. (1997). *Sambanden människa, teknik och organisation*. Studentlitteratur, Lund.
- VonWright, G. H. (1963). *Norm and Action*. London: Routledge & Kegan Paul.

Analysis of the Plant Modification Process at Forsmark Kraftgroup (AB FKA)

Johannes Petersen, Ørsted DTU

Introduction

In order to achieve a close interaction between the theoretical work and practice from the very beginning of the NKS project “Barrier, Control and Management” we have decided to focus on a specific aspect of safety work at nuclear power plants, namely the plant modification process.

This report reviews the plant modification process and the associated safety review process as described in the Forsmarks Kraftgrupp AB (FKA) documentation.

In order to achieve a preliminary picture of the interplay between the activities in the plant modification process and the activities in the review process we have tried to apply SADT (or IDEF0). Please note that SADT is not seen as the solution, but merely as a useful modeling methodology that can provide some valuable insight in the early phase of the project. The use of SADT could also help pinpoint specific modeling problems related to safety.

Documentation from FKA

In July we visited Olle Andersson at Forsmark and received documentation that is relevant for the plant modification process.

- 1) Management and Quality Handbook (Lednings- och kvalitetshandbok)
 - LOK 1.3 Management philosophy (Ledningsfilosofi)
 - LOK 2.3 Safety Reviewing (Säkerhetsgranskning)
 - LOK 2.6 Organization (Organisation)
 - LOK 3 Quality Requirements (Kvalitetskrav)
- 2) MTO Activities (MTO-Verksamhet) (FKA-I-126)
- 3) Forsmark Safety Reviewing (Forsmark – Säkerhetsgranskning) (F-I-824)
- 4) Instructions for plant modifications
 - Forsmark ordering instruction (Forsmark – Beställarinstruktion) (F-I-274)
 - Plant modification process; realization of plant modifications (Process anläggningsförnyelse – genomförande av anläggningsändring) (F-I-261)
 - Plant modification process (Process anläggningsförnyelse) (F-I-259)
- 4) Plant modification case:
 - Forsmark 1 and 2 System 321. Preventive measures for valves 321 V3-V4
 - Plant modification specification (F2-2002-30)
 - Review of specification (FQ-2002-182)
 - Statement from primary safety review (F2D-2002-46)

- Primary safety review (F1-2002-82)
- Plant modification specification (F2-2002-30) (revision)
- Plan for implementation (FT-2002-406)
- Primary safety review of plan for implementation (F1C-2002-26)
- Review of plan for implementation (FQ-2002-309)
- Plan for implementation (FT-2002-406 rev.1)
- FKA safety committee (2002-818)

The plant modification process

Plant modifications concern all rebuilding, modifications and new plant activities with interventions that modify the physical design or the properties of the plant in a way that requires a change in plant documentation or that these are complemented (F-I-259).

The plant modification process consists of two sub-processes, 1) inventory and initiation, performed by the ordering unit and 2) plant modification (preplanning, design, implementation and completion) performed by the project management function. An overview of the plant modification process is given in Figure 1.

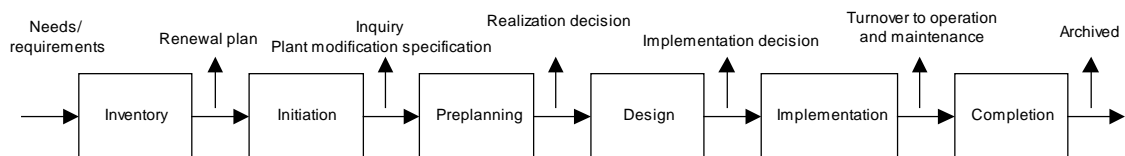


Figure 1. The plant modification process (adapted from F-I-261).

Modification initiatives (förslag till ändring)

Proposals for modification are collected from basically all work processes, they are scrutinised and reacted on. If they are accepted they are moved to the inventory of future modifications.

Inventory (inventering/prioritering)

Inventory and prioritizing of possible modifications is done by the ordering unit. The result is a continuous renewal plan with at least a 5 years perspective.

Initiation (initiering)

The initiation of plant modifications is normally based on the renewal plan and results in an inquiry for implementation.

Normally the plant modification is being specified in a *plant modification specification* by the ordering unit. The plant modification specification forms the basis for the inquiry for implementation.

Preplanning (förprojektering)

The preplanning is performed by the project management function. The preplanning is based on the inquiry and includes planning of implementation with respect to cost, time plan and quality. The project plan is done in collaboration with the ordering unit and internal suppliers.

Design (projektering)

During the design phase the following is performed: construction, planning of implementation, writing V&V documentation for the implementation and commissioning, delivery of equipment and components, education of personnel. An *implementation plan* is created.

Implementation (införande)

During implementation the project management function supervises the installation and testing (V&V). The ordering unit is responsible for the commissioning. After approved commissioning tests, the modification is turned over to the operating unit for operation and maintenance. The turnover is documented in a protocol.

Completion (avslut)

Project management supervises that possible remaining aspects are taken care of and that the plant documentation is adjusted accordingly.

Safety review process

The plant modification process is closely associated with a safety review process that is supposed to verify that all safety aspects are taken into account, that applicable norms and requirements are met and that sufficient account of factors concerning Human-Technology-Organization (MTO) is taken. The safety review process at Forsmark is described in F-I-824.

There are basically two types of safety reviews: 1) primary safety review and 2) independent safety review. Section 6 in F-I-824 provides general guidelines for safety review and section 7 shows a collection of requirements against which a review must be performed.

Primary safety review

The purpose of the primary safety review is to ensure that all safety and quality requirements are taken into consideration.

The primary safety review is performed by the unit responsible for the given factual matter. That means that the production units and FG are responsible for the primary safety review with respect to precondition for plant operation. Other units can be involved to ensure coverage of required specialist knowledge (e.g. the technical unit, FT and the maintenance unit, FM).

The primary safety review shall be documented. From the documentation it must be evident:

- What has been reviewed.
- Who has performed the review.
- Whether all relevant safety aspects have been addressed.
- A standpoint on whether the safety assessment has been performed satisfactory.
- How the review has been performed (review against requirements in FSAR, control calculations, etc.).
- A standpoint on the applied methods, etc.
- Other comments.

It must be documented how the review aspects are taken into consideration. For plant modifications this must be documented in the *plant modification specification*, *implementation plan* and *project report*.

Independent safety review

The purpose of the independent safety review is to control and verify that the applicable safety aspects are taken into account and that safety requirements for factual matters are met. This is done without any time and cost constraints.

In order to ensure the independent nature of the safety review the persons performing the review must not be involved in suggesting solutions or other kind of activities that might otherwise question the independent nature of the review. The independent safety review is performed by FQ.

The independent safety review shall be documented. From the documentation it must be evident:

- What has been reviewed
- Who has performed the review
- A stand on the safety judgment and that safety aspects have been treated satisfactory
- Other comments

It must be documented how the review aspects are taken into consideration. For plant modifications this must be documented in the *plant modification specification*, *implementation plan* or in a *project report*.

Review groups

The review process is performed differently depending on the type of plant modification in question. There are three different safety review groups (F-I-824). The purpose of having different review groups is to direct resources to the modifications that are most important to safety.

The decision order for plant modifications in review group 1 is shown schematically in Figure 2.

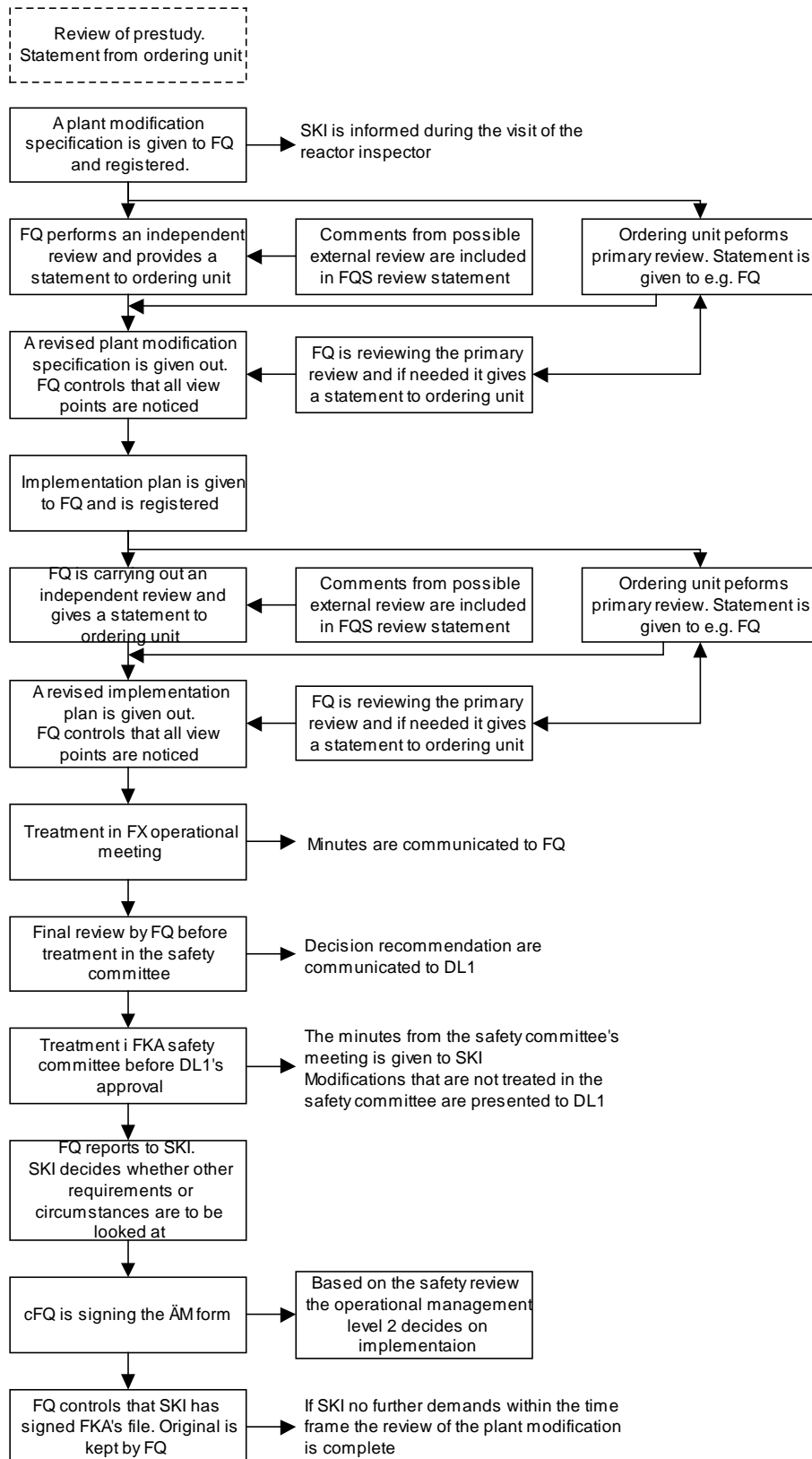


Figure 2. The review process in review group 1 (adapted from F-I-824).

The safety review of plant modifications in review group 1 is based on a plant modification specification and an implementation plan.

Before the primary safety review the concerned unit shall provide a statement, appointed by the operational management level 2, that must be communicated to FQ. Before the independent safety review FQ shall give a review statement to the units responsible for the factual matter, normally the ordering unit(s).

The primary safety review is controlled by instructions. From these instructions it has to appear:

- Who are responsible for performing the primary safety review.
- Who must carry out the different parts of the review and how this is administrated
- Who appoints the primary safety review
- Qualifications for those who perform the primary safety review

FQ is responsible for informing SKI about ongoing plant modifications already in the early phases of the project.

After finishing the review process the plant modification specification and the implementation plan are fixed. From the respective documents it must appear how the statements from the safety unit and the primary safety review have been taken into account.

After the plant modification specification and the implementation plan have been fixed FQ reviews whether all relevant review comments have been taken into consideration. FQ also reviews the extent, quality and depth of the primary safety review. If required, a written statement is given to the unit concerned and the plant modification specification and implementation plan will have to be revised accordingly

The unit concerned by the modifications shall notify FQ in a written statement about modifications before the treatment in the FKA safety committee. Before notice to bring the matter to the safety committee the topics must have been approved by the ordering unit. This is normally performed in a FX – operational meeting.

Before the treatment in the safety committee FQ performs a final review of left over topics and provides a recommendation for operational management level 1 (DL1) decision. DL1 approves modifications in review group 1 on the basis of the minutes from the safety committees meeting.

Before a modification can be implemented SKI must be notified. SKI decides whether additional or other requirements should be imposed on the modification. The decision about whether to implement a modification or not must be taken after notifying SKI. FKA, however, does not have to await SKI's answer.

After the FKA's safety review the cFQ signs the Modification Form (ÄM).

An integrated model of the plant modification process and the safety review process

In this section a preliminary and partial version of an integrated model of the plant modification process and the safety review process is described. We use the system description method SADT (Structured Analysis Design Technique) also known as IDEF0 (see e.g. (Marca and McGowan, 1988)).

SADT provides the possibility to model system *activities* or *processes* at different levels of decomposition. Furthermore, it defines the relationship among these activities through the *things* of the system.

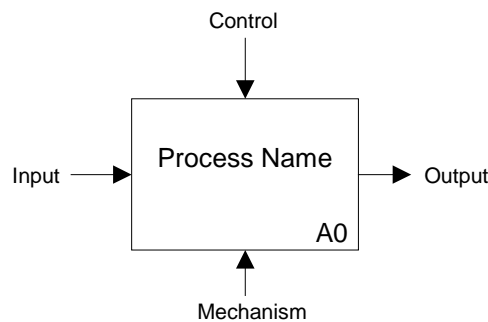


Figure 3. An SADT/IDEF0 box.

The SADT boxes represent a function or an active part of the system. Each side of SADT box has a specific meaning. The left side of the box is reserved for *inputs*, the top side is reserved for *controls*, the right side is reserved for *outputs*, and the bottom side is reserved for *mechanisms*. This notation represents certain system principles: inputs are transformed into outputs, controls constrain or dictate under what conditions transformations occurs.

Figure 4 shows a partial SADT model of the plant modification process (including the safety review process). Note that only two phases of the plant renewal process are considered: *initiation* and *preplanning*.

It can be seen that the initiation process (A1) produces a preliminary plant modification specification. This preliminary plant modification specification is reviewed by an independent safety review (A2) and a primary safety review (A3). Eventually the primary safety review is reviewed by FQ (A4). The output of A2, A3 and A4 controls the preparation of the revised plant modification specification. The revised plant modification specification serves as an input for the preplanning process (A5).

After the *planning* phase (not shown) the pattern of review process is repeated. This time the object of the review process is the implementation plan.

Each of the processes in Figure 4 is controlled by norms, requirements and instructions. In order to capture the complete picture also the processes that lead to changes in norms, requirements and instructions should have been included. As an example of a change in

the instructions one could mention the introduction of MTO aspects. The processes that lead to changes in norms, requirements and instructions seem, however, to be less well-documented (for good reasons).

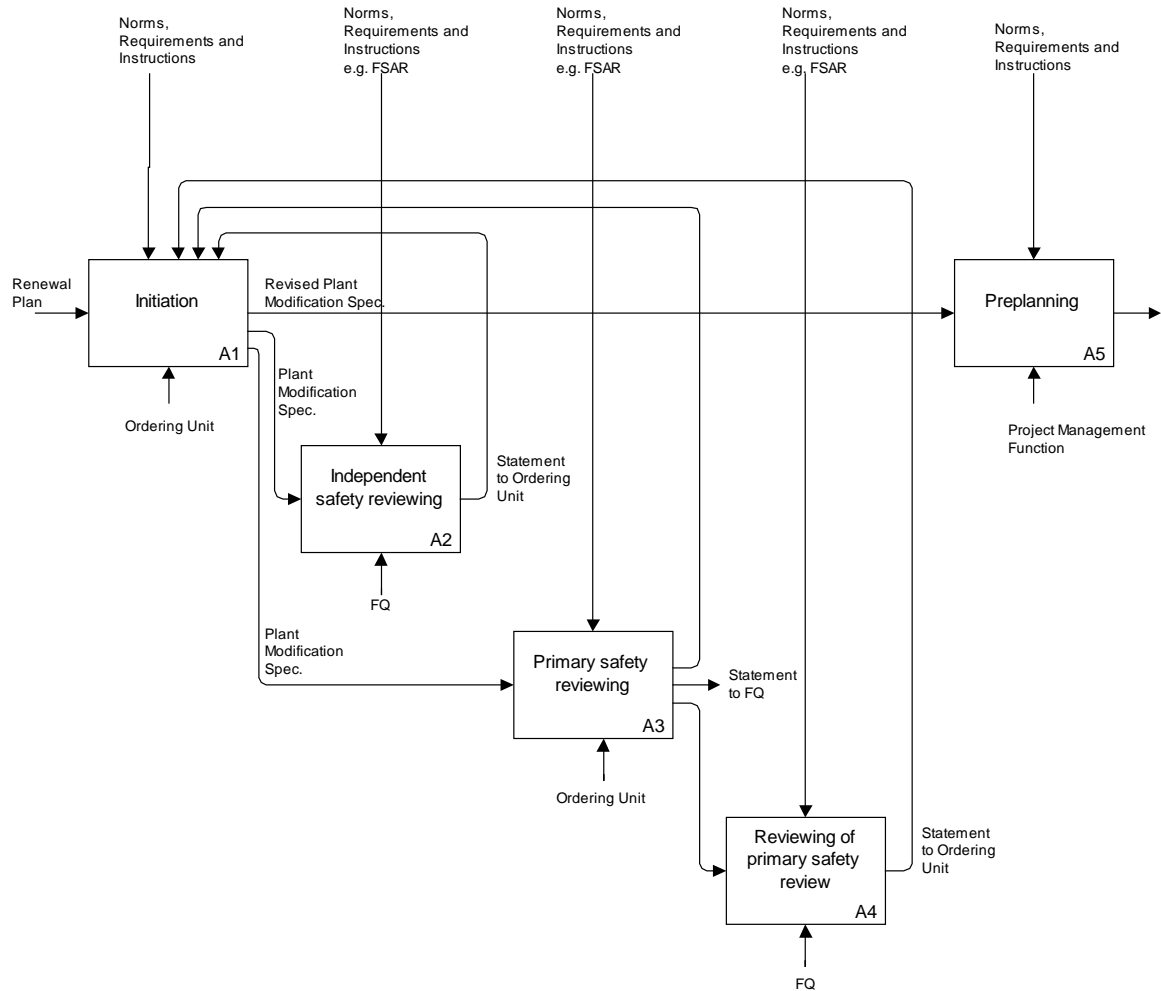


Figure 4. A SADT model of parts of the plant modification process - including the review process.

Acknowledgements

The author would like to thank Björn Wahlström (VTT) and Olle Andersson (FKA) for many helpful comments on earlier versions of this report.

References

Marca, D.A. and McGowan, C.L. (1988). *SADT. Structured analysis and design technique*. McGraw-Hill Book Inc., New York.

Modeling Plant Modification Processes Using Von Wright's Action Concepts

Johannes Petersen, Ørsted DTU

Introduction

This report describes a preliminary attempt to use Von Wright's generic action and change types to model the prescribed activities of the plant modification process and the associated safety review process at nuclear power plants. In order to model the means-end structure of the activities advantage is taken of some of the concepts and relations defined for Multilevel Flow Modeling (MFM) (Lind, 1999).

The report focuses on a subset of activities in the plant modification process at Forsmark Kraftgrupp (AB FKA) (Petersen, 2003a): 1) generation of the plant modification specification, 2) primary safety review of the plant modification specification, and 3) revision of the plant modification specification.

The report outlines Von Wright's logic of action, as described in (Lind, 2003). Furthermore, it discusses the difference between descriptive and prescriptive descriptions of action - a distinction that is fundamental in order to understand how function descriptions differ from descriptive action descriptions. Following an introduction to the relevant concepts and relations from Multilevel Flow Modeling means-end models of the individual plant modification and review activities based on Von Wright's generic actions are described. Finally, an integrated model capturing the dependencies between the activities is proposed.

Von Wright's logic of action

Von Wright has proposed a set of generic and elementary action types based on a set of elementary changes that can happen in the environment (Lind, 2000).

Change Schema and Change Description

The changes are specified using the generic proposition p and the associated truth value. Lind (2003) makes a distinction between *change schemas* and *change descriptions*. Change schemas describe the logic structure of elementary changes based on the generic proposition p describing the state of affairs and the operator T (then). An example of a change schema is $pT\sim p$, expressing that first p is true and *then* $\sim p$ is true. The corresponding change description is ' p happens'. Note that a non-change such as pTp is also considered a change.

Action Schema and Action Description

Lind (2003) also makes a distinction between *action schemas* and *action descriptions*. Action schemas express the logic structure of elementary actions based on the two operators T (*then*) and I (*instead*), whereas the action description expresses the meaning of an action schema. The action schema includes the *initial state*, the *result* of the agent intervening and the *counterfactual result* that would have happened had the agent not intervened:

$\langle \text{action-schema} \rangle := \langle \text{initial-state} \rangle T (\langle \text{result} \rangle I \langle \text{counterfactual-result} \rangle)$

An example of an action schema is $pT[\sim pIp]$, expressing that first p is true (the initial state) *then* $\sim p$ is true (the result) *instead of* p being true (the counterfactual result). Had the agent not intervened then p would have remained true. The corresponding action description is ‘destroy p ’. Table 1 contains a description of the elementary changes and actions (interventions)³.

Change	Action Schema	Action Description
$\sim pT p$ p happens	$\sim pT[pI\sim p]$	produce p
$pT p$ p remains	$pT[pI\sim p]$	maintain p
$pT\sim p$ p disappears	$pT[\sim pIp]$	destroy p
$\sim pT\sim p$ p remains absent	$\sim pT[\sim pIp]$	suppress p

Table 1. Changes and interventions.

Von Wright’s elementary actions implicitly presume the existence of an antagonist that counteracts the agent (Lind, 2003). The antagonist denotes the inherent nature (dynamics) of the environment with which the agent interacts. When the agent does not intervene the antagonist determines the development of the state of the environment. This means that the agent can omit to intervene (also an action) if the antagonist results in a development of the state of the environment that corresponds to the goal of the agent.

Covert and overt aspects of actions

According to Lind (2003), Von Wright is only concerned with the overt aspects of action, i.e. what the agent does, and not the covert aspects such as the intentions for acting.

In order to make explicit the covert aspects of an action Lind (2003) has proposed to let the action descriptions express the intentions behind an action, while letting the action schemas express the overt aspect of actions. This is a possibility because the action descriptions shown above are logical redundant with respect to the action schemas, e.g. ‘produce p ’ is logically equivalent to ‘destroy $\sim p$ ’ and ‘maintain p ’ is logically equivalent to ‘suppress $\sim p$ ’. Thus for each intervention described by some action schema there is a pair of logical redundant action descriptions. According to Lind (2003) one of these actions is a *promote* action, promoting the happening of a specific state in the environment, while the other one is an *oppose* action, opposing the happening of a specific state in the environment. Produce and maintain denote promote actions, while destroy and suppress are oppose actions.

³ Apart from interventions Von Wright discusses also omissions. The set of elementary omissions is not shown in Table 1.

Action Schema	Promote action	Oppose action
$\sim pT[pI\sim p]$	produce p	destroy $\sim p$
$pT[pI\sim p]$	maintain p	suppress $\sim p$
$pT[\sim pIp]$	produce $\sim p$	destroy p
$\sim pT[\sim pIp]$	maintain $\sim p$	suppress p

Table 2. Promote and oppose actions.

Consequently, the distinction between promote and oppose actions are used to make explicit the intention behind specific actions. That is, for the action described by the action schema $pT(pI\sim p)$ the intention of the agent might be to ‘maintain p’, referring to the state that is promoted (p), or ‘suppress $\sim p$ ’, referring to the state that is opposed ($\sim p$).

Actions and Functions

Hitherto a *descriptive* perspective on actions has been assumed, focusing on what an agent actually does. An agent, however, may be ascribed a function by some indirect agency, meaning that it is supposed to act in a specific way (Lind, 2000). A description of what the agent is supposed to do (its function) corresponds to a *prescriptive* perspective on actions.

Although Von Wright tends to focus on animate (human) agents manipulating a dynamic physical environment there seems to nothing that hinders an application of Von Wright’s action concepts to inanimate agents also.

An agent having a function can be both animate (e.g. a person or an organization) and inanimate (e.g. a physical component or a system).

A descriptive perspective on action

When adopting a descriptive perspective on action the focus is on describing what an agent *in fact* does (the overt aspect) and what the agent *intends* to do (the covert aspect). The overt aspect is expressed by an action schema (e.g. $\sim pT[pI\sim p]$), whereas the covert aspect is expressed by an action description that corresponds to the given action schema (e.g. ‘produce p’ or ‘destroy $\sim p$ ’).

Note that, from a descriptive perspective, it is not meaningful to talk about the covert aspects of an action (intentions) for inanimate agents, since this type of agent cannot have intentions.

A prescriptive perspective on action

An agent can be ascribed a function, meaning that it is supposed to perform a specific action. Due to the fact that a function is an ascribed property it is characteristic that an agent which is ascribed a specific function will have this function no matter whether it actually performs the prescribed action or not (the latter corresponds to a malfunction).

When adopting a prescriptive perspective on action the focus is on describing what an agent *is supposed to do* (overt aspect) and what is the *goal* (covert aspect). Also for

prescriptive action descriptions action schemas and action descriptions are used to express the overt and covert aspect, respectively.

From a prescriptive perspective it is meaningful to talk about overt and covert aspects of the actions of both animate and inanimate agents. Table 3 summarizes the meaning of *action descriptions* (capturing the covert aspect of an action) and *action schemas* (capturing the overt aspect of an action) for descriptive and prescriptive perspectives on action.

	Descriptive perspective	Prescriptive perspective
Overt aspects	An action schema expressing the difference that the action of an agent <i>in fact</i> makes in the environment (for both animate and inanimate agents).	An action schema expressing the difference that the action of an agent <i>is supposed to</i> make in the environment, i.e. its function (for both animate and inanimate agents).
Covert aspects	An action description expressing the intention of the agent (only for animate agents)	An action description expressing the goal ascribed to the agent by some indirect agency (for both animate and inanimate agents).

Table 3. Aspects of action from a descriptive and a prescriptive perspective.

Modeling the means-end structure of a set of functions

Above it has been argued that it is possible to use Von Wright’s action concepts to describe the goals and functions of some agent (either animate or inanimate). In order to capture the means-end structure of a set of functions, e.g. of a physical system or an organization we need to define a set of concepts and relations. Here we will use concepts and relations that are similar to those of Multilevel Flow Modeling (Lind, 1999).

Concepts

A *goal* describes the intended outcome of an action/activity. As already suggested above *action descriptions* such as ‘produce p’ or ‘maintain r’ can be used as goal expressions. The actual content of a goal depends on a specification of the propositions p and r.

A *function* describes the role that an agent has in the achievement of one or several goals. A function of an agent can be expressed by *action schemas* such as $\sim pT(pI\sim p)$ or $pT(pI\sim p)$.

An *agent* realizing a function can be both animate (a person or an organization) and inanimate (a physical component or a system).

Relations

Goals, functions and agents can be described at different levels of decomposition (part-whole). When a function is decomposed into a set of sub-functions it is characteristic that there are some dependencies among the sub-functions, e.g. input-output, etc. Below a set of means-end relations, adapted from MFM (Lind, 1999), is described.

The achieve relation

The achieve relation relates a goal to the function(s) that is supposed to achieve it.

The condition relation

In order to enable a function a set of preconditions typically needs to be satisfied. Such preconditions may relate to the capability of the agent performing the function or the capability of the patient(s) undergoing a change or being transformed. This can be expressed by the condition relation connecting a function to the goal that should be satisfied in order to enable the function.

The realize relation

The realize relation expresses the link between a functions and the agent(s) realizing it.

The mediate relation

Sometimes when an agent acts on a specific object it acts also on another object (at the same time). E.g. when transporting water the energy contained in the water is also transported. From a functional point of view the agent uses the former object as a medium for acting on the latter object. What the agent does can be described by two related functions focusing on the direct and the indirect object, respectively. The relation between such functions can be expressed by the mediate (M) relation.

The producer-product relation

Another common feature of action is that the doing of one thing can have different interpretations corresponding to a change in the perspective from the doing itself to the product being produced (also an action). This gives rise to two alternative but related function descriptions focusing on the process and the product, respectively. The relation between such functions can be expressed by the so-called producer-product (PP) relation.

Sometimes it is difficult to determine whether an action of some agent is actually producing another action or whether it is only stimulating the performance of another action (realized by another agent). It is only appropriate to use the PP-relation in the former case.

Relation	Symbol	Explanation
Achieve	A	Represents the relation between a goal (end) and the function (the means) used for its achievement.
Condition	C	Represents a relation between a function and a goal that should be satisfied in order to enable the function.

Realize	R	Represents a relation between a function and the physical components or subsystems that implement the function.
Mediate	M	Represents the relation between a function and a process that mediates it.
Producer-product	PP	Represents the relation between a function (the product) and a process (the producer) that brings it about.

Table 4. The graphical symbols and descriptions of the relations used to capture the means structure of a set of functions. Adapted from (Lind, 1999).

The plant modification process

Plant modifications have to do with modifications in the physical design or the properties of a nuclear power plant. The rationale for making plant modifications relates to one or more of the following aspects:

- increased or improved safety (reactor safety, industrial safety, environmental safety).
- increased accessibility and efficiency.
- improvements with respect to plant operation and maintenance.
- lack of spareparts (requiring new types of components).

Whenever it is decided to perform a plant modification the plant modification process is initiated. The plant modification process at Forsmark consists of a sequence of phases where the output of one phase is the input to the next (see (Petersen, 2003a) for an overview).

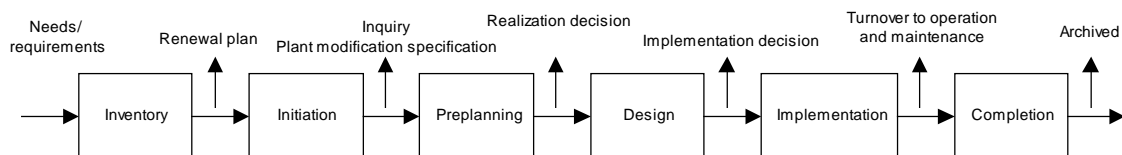


Figure 5. An overview of the plant modification process. Adapted from (F-I-261).

The initiation phase consists of two sub-phases, which we may refer to as the *generation* and the *revision* phase. In the *generation* phase the *plant modification specification* is produced and in the *revision* phase the plant modification specification is revised. Before the revision phase is initiated the plant modification specification is *reviewed*. There are three types of reviews: an independent safety review, a primary safety review, and a review of the primary review. Here we focus on the primary safety review.

Modeling three types of functions of the ordering unit in the initiation phase

Function_1: Generation of the plant modification specification

The generation phase is viewed as a function realized by the ordering unit. In order to apply Von Wright's action concepts it is necessary specify meaningful states of the environment with which an agent can interfere.

If we consider the state p = "the plant modification specification is available" then the goal of the generation function can be expressed by the action description 'produce p ' emphasizing that the goal is to promote p . The generate function can be described by the action schema $\sim pT[pI\sim p]$. This expresses the initial state ($\sim p$), the result (p) and the counterfactual result ($\sim p$). The means-end structure of the generate process is shown in Figure 6.

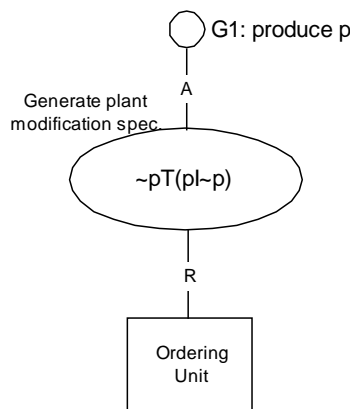


Figure 6. The function of the generate process, achieving the goal $G1$ and realized by the ordering unit.

Function_2: Primary safety review of the plant modification specification

A safety review can be understood as an evaluation activity that is supposed to generate information about some property (e.g. the quality) of the object being reviewed (e.g. the plant modification specification) with respect to some norms and requirements.

Note that a review process is an act of information processing. This type of action is different from actions manipulating physical objects. Although Von Wright has focused mainly on the latter type of action, his action concepts may also be used to describe actions of information processing.

The primary safety review is supposed to generate information about possible discrepancies between the content of the plant modification specification and the safety and quality requirements. The primary safety review is performed by the ordering unit.

If we consider the state q = "information about the discrepancies between the content of the plant modification specification and the safety and quality requirements is available"

the goal of the safety review can be expressed by the action description ‘produce q ’ (emphasizing that the goal is to promote q). The review function is described by the action schema $\sim qT[qI\sim q]$. The means-end structure of the review process is shown in Figure 7.

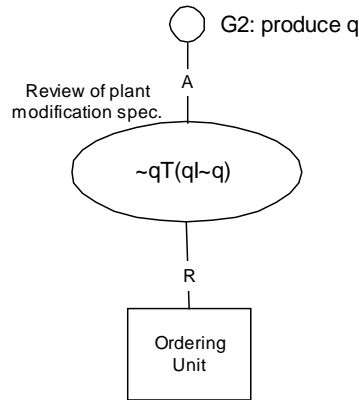


Figure 7. The function of the review process achieving the goal G2 and realized by the ordering unit.

Function_3: Revision of the plant modification specification

The revision process manipulates the plant modification specification based on information about the discrepancies produced by the review process. Its function is to eliminate the existence of discrepancies between the content of the plant modification specification and the safety and quality requirements. The revision process is performed by the ordering unit.

Based on the state r = “discrepancies between the content of the plant modification specification and the safety and quality requirements exist” the goal of the revision process can be expressed by the action description ‘destroy r ’ (emphasizing that the goal is to oppose r). The revision function can be described by the action schema $rT[\sim rI r]$. The means-end structure of the revision process is shown in Figure 8.

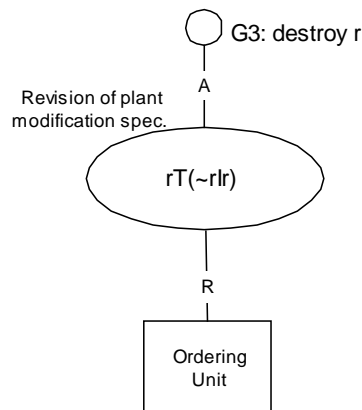


Figure 8. The function of the revision process achieving the goal G3 and realized by the ordering unit.

A model of the means-end structure of the functions of the ordering unit in the first phase of the plant modification process

To summarize, we have specified three functions of the ordering unit in the first phase of the plant modification process:

- 1) $\sim pT[pI\sim p]$ (generation of the plant modification specification)
- 2) $\sim qT[qI\sim q]$ (primary safety review) and
- 3) $rT[\sim rIr]$ (revision of the plant modification specification)

The state descriptions for p , q and r are:

p = “the plant modification specification is available”

q = “information about the discrepancies between the content of the plant modification specification and the safety and quality requirements is available”

r = “discrepancies between the content of the plant modification specification and the safety and quality requirements exist”

Before we describe the overall means-end structure of the functions we would like to suggest yet another function with the goal to suppress that errors of the plant modification specification is handed over to the project management function (the units responsible for carrying out the subsequent phases of the plant modification process). In order to do this we define yet another state:

s = ”errors in the plant modification specification when handed over to the project management function exist”.

The function is described by the action schema $\sim sT[\sim sIs]$ and the goal is described by the action description ‘suppress s ’.

Figure 9 shows a model of the overall means-end structure of the functions of the ordering unit in the initiation phase of the plant modification process. Refer to the previous section for a description of the individual functions.

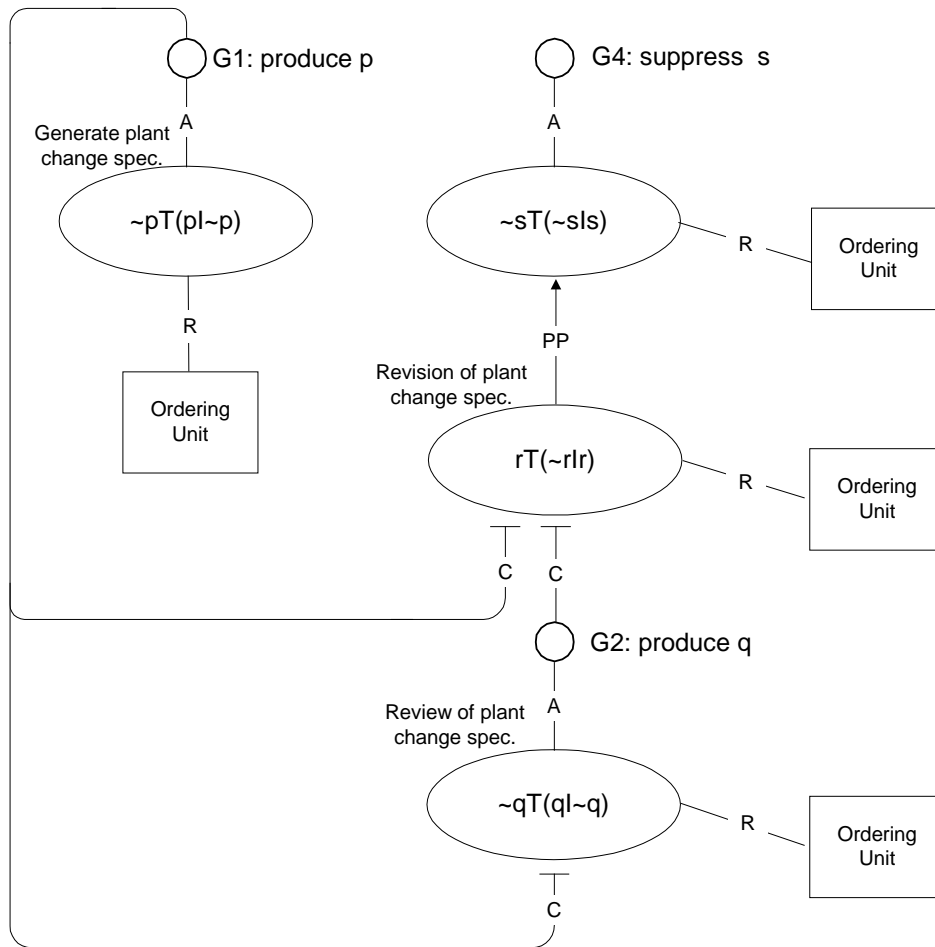


Figure 9. A model of the overall means-end structure of the functions of the ordering unit in the initiation phase of the plant modification process.

The goals G1 ‘produce p’ and G4 ‘suppress s’ are achieved by the functions $\sim pT[pI\sim p]$ and $\sim sT[\sim sIs]$ respectively.

It can be seen that the function $\sim sT[\sim sIs]$ is *produced* by the function $rT[\sim rIr]$ (revision process). In turn there are two conditions on the $rT[\sim rIr]$ function expressed by the goals G1 and G2 respectively. G1 is achieved by the function $\sim pT[pI\sim p]$ and G2 is achieved by the function $\sim qT[qI\sim q]$. Furthermore the function $\sim qT[qI\sim q]$, achieving G2, is conditioned by the goal G1.

Note that the ordering unit realizes all the functions in Figure 9.

Conclusions

The report has presented a preliminary attempt to apply Von Wright’s generic action and change types to model the prescribed activities of the plant modification process and the associated safety review process at nuclear power plants.

Concepts and relations from Multilevel Flow Modeling (MFM) have been used to model the means-end structure of the activities.

The present modeling results have illustrated that Von Wright's logic of action is useful for the modeling of safety activities. It is obvious, however, that more work needs to be done in order to integrate properly Von Wright's concepts with MFM. More specifically, it is necessary to clarify the distinction between the different categories of means and ends proposed by Lind (1993). This topic will be investigated in the main phase of the project.

Acknowledgements

The author would like to thank Björn Wahlström (VTT) and Olle Andersson (FKA) for helpful comments on earlier versions of this report.

References

- Lind, M. (1993). Functional Architectures for Systems Management and Control. In: Lind, M. et al., Interactive Planning for Integrated Supervision and Control in Complex Plant. Final report from CEC JRC project 4937-92-08-ED ISP DK.
- Lind, M. (1999). *Plant modelling for supervisory control*. Trans Inst MC, Vol. 21. No. 4/5, pp. 171-180.
- Lind, M. (2000). *Actions, functions and failures in dynamic environments*. Center for Human-Machine Interaction. Report CHMI-8-2000.
- Lind, M. (2003). *Promoting and Opposing. A Semantic analysis of Von Wright's action types*. In: NKS project NKS-R-07: Barriers, Control and Management- Report from the pilot phase (this report).
- Petersen, J. (2003a). *Analysis of the Plant Renewal Process at Forsmark Kraftgroup (AB FKA)*. In: NKS project NKS-R-07: Barriers, Control and Management- Report from the pilot phase (this report).
- (F-I-261). Plant modification process; realization of plant modifications (Process anläggningssförnyelse – genomförande av anläggningsändring). Forsmark kraftgroup (AB FKA).

Title	Barriers, Control and Management. Report from the pilot phase
Author(s)	Morten Lind
Affiliation(s)	Technical University of Denmark
ISBN	87-7893-145-2
Date	September 2003
Project	NKS-R-07
No. of pages	48
No. of tables	16
No. of illustrations	15
No. of references	33
Abstract	<p>The report documents the results of the pilot phase of the NKS project "Barriers, Control and Management" (NKS-R-07). The following conclusions can be drawn for the work done in the pilot phase:</p> <ul style="list-style-type: none">• A set of research issues and hypotheses to be developed in the main phase of the project has been defined.• The theoretical work has led to a clarification of the semantic distinctions between safety related actions, control actions and barriers.• The action concepts of Von Wright have been applied on a case study on the nuclear power plant in Forsmark, Sweden. It has been shown that it is possible to apply the concepts. But it is also concluded that extensions of the theory are required. Such extensions are important objectives for the main phase of the project.
Key words	Formalized concepts, action, function, consistency, procedures, documents