

# CAST 핸드북:
# 사건과 사고로부터 더 많은 것을 배우는 방법
# (How to Learn More from Incidents and Accidents)

Nancy G. Leveson

영문/한글판 v1.0

Translated by TTA (supported by Ministry of Science and ICT)

과학기술정보통신부 Ministry of Science and ICT

TTA 한국정보통신기술협회 Telecommunications Technology Association

COPYRIGHT © 2019 BY NANCY LEVESON. ALL RIGHTS RESERVED. THE UNALTERED VERSION OF THIS HANDBOOK AND ITS CONTENTS MAY BE USED FOR NON-PROFIT CLASSES AND OTHER NON-COMMERCIAL PURPOSES BUT MAY NOT BE SOLD.

본 핸드북은 과학기술정보통신부의 “SW공학경쟁력강화” 사업의 결과물입니다.



과학기술정보통신부
Ministry of Science and ICT



한국정보통신기술협회
Telecommunications Technology Association

An accident where innocent people are killed is tragic,
but not nearly as tragic as not learning from it.

무고한 사람들이 목숨을 잃는 사고는 비극적이다.
그러나 그것으로부터 배우지 않는 것이 더 비극적이다

# Preface

About 15 years ago, I was visiting a large oil refinery while investigating a major accident in another refinery owned by the same company. The head of the safety engineering group asked me how they could decide which incidents and accidents to investigate when they had hundreds of them every year. I replied that I thought he was asking the wrong question: If they investigated a few of them in greater depth, they would not have hundreds. I don't think he understood, or at least did not accept, my suggestion. The goal of this handbook is to explain that answer—we are not learning enough from the incidents and accidents we are having. We need to figure out how to learn more if we truly want to significantly reduce losses.

After working in the field of system safety and helping to write the accident reports of several major accidents (such as the Space Shuttle Columbia, Deepwater Horizon, and Texas City) and other smaller ones, I have found many factors common to all accidents. Surprisingly, these are often not included as a cause in the official accident reports. CAST (Causal Analysis based on System Theory) and this handbook are my attempt to use my experience to help others learn more from accidents in order to do a better job in preventing losses in the future.

The handbook describes a structured approach, called CAST (Causal Analysis based on System Theory), to identify the questions that need to be asked during an accident investigation and determine why the accident occurred. CAST is very different than most current approaches to accident analysis in that it does not attempt to assign blame. The analysis goal changes from the typical search for failures to instead look for why the systems and structures in place to prevent the events were not successful. Recommendations focus on strengthening these prevention (control) structures, based on what was learned in the investigation.

How best to perform CAST has evolved with my experience in doing these analyses on real accidents. Updates to this handbook will provide more techniques as all of us learn more about this systems approach to accident analysis.

**Acknowledgements:**
I would like to thank several people who helped to edit this handbook: Dr. John Thomas, Andrew McGregor, Shem Malmquist, Diogo Castilho, and Darren Straker.

# 머리말

약 15년 전, 나는 대형 정유 공장을 방문하였는데 이 때 동일 회사의 다른 정유 공장에서 발생한 큰 사고를 조사하는 중이었다. 안전 부서의 책임자는 매년 발생하는 수백 건의 사건(incident)과 사고(accident) 중 어떤 것을 조사할지 어떻게 결정하느냐고 나에게 물었다. 나는 그가 잘못된 질문을 하고 있는 것 같다고 대답했다: 만약 그들이 사고 중 일부를 훨씬 더 깊이 조사했다면 실제로는 수백 건의 사고가 아닐 수 있다. 나는 그가 내 의견을 이해하지 못했거나 적어도 받아들이지 않았던 것 같다. 이 핸드북의 목표는 우리가 겪고 있는 사건과 사고로부터 충분하게 배우고 있지 않다는 것을 설명하는 것이다. 우리는 진정 사고로 인한 손실을 크게 줄이고 싶다면 더 많은 것을 배울 수 있는 방법을 찾아야 한다.

시스템 안전 분야에서 일하고 여러 중대사고(우주왕복선 컬럼비아, 딥워터 호라이즌, 텍사스 시티 등)나 비교적 작은 규모 사고의 사고 보고서 작성을 지원하면서, 많은 요인들이 모든 사고에서 공통적임을 발견했다. 하지만 놀랍게도, 이 요인들은 종종 공식 사고 보고서에서 사고 원인에 포함되지 않고 누락되었다. CAST(Causal Analysis based on System Theory)와 본 핸드북은 사람들이 사고로부터 더 많은 것을 배워 미래의 손실을 예방하는데 더 나은 역할을 할 수 있도록 나의 경험을 토대로 만들어진 것이다.

본 핸드북에서는 사고 조사 중 필요한 질문들을 찾아내고 사고의 원인을 파악하기 위해서 CAST(Causal Analysis based on System Theory)라 불리는 구조화된 접근법을 설명한다. CAST는 사고에 대한 책임 소재를 따지지 않는다는 점에서 대부분의 현 사고 분석 접근법과 큰 차이가 있다. 사고 분석의 목표가, 실패를 찾아내는 전형적인 방식에서 이벤트 방지를 위해 시스템과 컨트롤 스트럭처가 제대로 작동하지 않은 이유를 찾는 것으로 변화하였다. 권고사항들은 이러한 예방 (컨트롤) 스트럭처를 강화하는 것에 초점이 맞추어져 있으며, 이는 조사 과정에서 알게 된 것에 근거한 것이다.

나는 실제 사고를 분석했던 경험을 통해 CAST를 수행하는 최적의 방법을 발전시켜 왔다. 앞으로, 사고 분석에 대한 시스템적 접근 방식에 대해 더 알게 되는 것들을 핸드북에 업데이트하여 더 많은 기법들을 제공하고자 한다.

**감사의 말:**

이 핸드북을 편집하는 데 도움을 준 여러 분들께 감사의 말씀을 전합니다 : John Thomas, Andrew McGregor, Shem Malmquist, Diogo Castilho, Darren Straker.

**TABLE OF CONTENTS**

Prolog
1. Introduction
    - Why do we need a new accident analysis tool?
    - Goals of this handbook
    - What is CAST?
    - Relationship Between CAST and STPA
    - Format and Use of this Handbook
2. Starting with some Basic Terminology (Accident and Hazard)
3. Why aren't we Learning Enough from Accidents and Incidents?
    - Root Cause Seduction and Oversimplification of Causality
    - Hindsight Bias
    - Unrealistic Views of Human Error
    - Blame is the Enemy of Safety
    - Use of Inappropriate Accident Causality Models
    - Goals for an Improved Accident Analysis Approach
4. Performing a CAST Analysis
    - Basic Components of CAST
    - Assembling the Foundational Information
    - Understanding what Happened in the Physical Process
    - Modeling the Safety Control Structure (aka the Safety Management System)
    - Individual Component Analysis: Why were the Controls Ineffective?
    - Analyzing the Control Structure as a Whole
    - Reporting the Conclusions of the Analysis
    - Generating Recommendations and Changes to the Safety Control Structure
    - Establishing a Structure for Continual Improvement
    - Suggestions for Formatting the Results (will depend partly on industry culture and practices)
5. Using CAST for Workplace and Social Accidents
    - Workplace Safety
    - Using CAST for Analyzing Social Losses
6. Introducing CAST into an Organization or Industry

Appendix A: Links to Published CAST Examples for Real Accidents

Appendix B: Background Information and Summary CAST Analysis of the Shell Moerdijk Loss

Appendix C: The "Bad Apple" Theory of Accident Causation

Appendix D: Factors to Consider when Evaluating the Role of the Safety Control Structure in the Loss

Appendix E: Basic Engineering and Control Concepts for Non-Engineers

# 목 차


**머리말** ····· 3

**1장: 소개** ····· 6

왜 새로운 사고 분석 도구가 필요한가? ····· 6

이 핸드북의 목표 ····· 6

CAST란 무엇인가? ····· 7

CAST와 STPA의 관계 ····· 8

이 핸드북의 형식과 사용 ····· 8

**2장: 기본 용어(사고 및 위험)부터 시작하기** ····· 9

**3장: 사고(Accidents)와 사건(Incidents)으로부터 충분히 배우지 못하는 이유는 무엇인가?** ····· 12

근본 원인 부추기기 및 인과 관계의 지나친 단순화 ····· 12

사후 확신 편향(Hindsight Bias) ····· 14

인적 오류에 대한 비현실적인 시각 ····· 16

비난은 안전의 적 ····· 18

부적절한 사고 인과관계 모델의 사용 ····· 23

사고 분석 기법의 개선을 위한 목표 ····· 33

**4장: CAST 분석 수행** ····· 34

CAST의 기본 구성요소 ····· 34

기본 정보 수집 ····· 36

컨트롤드 프로세스에서 일어나는 일의 이해 ····· 41

안전 컨트롤 스트럭처(aka. 안전 관리 시스템) 모델링 ····· 46

개별 컴포넌트 분석 : 컨트롤이 왜 효과가 없었는가? ····· 55

전체로서의 컨트롤 스트럭처 분석 ····· 76

안전 컨트롤 스트럭처에 대한 권고사항 및 변경사항 작성 ····· 90

지속적 개선을 위한 구조 구축 ····· 90

CAST 결과 포맷 제안(일부 산업 문화 및 관행에 따라 다름) ····· 92

**5장: 작업장 및 사회적 사고에 대한 CAST 활용** ····· 98

작업장 안전 ····· 98

CAST를 활용한 사회적 손실 분석 ····· 103

**6장: 조직이나 산업에 CAST 도입** ····· 117

**부록A: 실제 사고에 대한 CAST 분석 발표 사례 링크** ····· 119

**부록B: 쉘 뫼르딕(Shell Moerdijk) 손실의 배경 정보 및 CAST 분석 요약** ····· 121

**부록C: 사고 원인에 대한 "썩은 사과(Badd Apple)" 이론** ····· 133

**부록D: 손실에서 안전 컨트롤 스트럭처의 역할을 평가할 때 고려해야 할 요소** ····· 136

**부록E: 비엔지니어를 위한 기본적인 엔지니어링 및 컨트롤 개념** ····· 140

**TABLE OF FIGURES**


1. Root Cause Seduction leads nowhere.
2. Playing Whack-a-Mole
3. A graphical depiction of hindsight bias.
4. The Following Procedures Dilemma
5. Two opposing views of accident explanation
6. Heinrich's Domino Model
7. Reason's Swiss Cheese Model
8. Emergent properties in system theory
9. Controllers enforce constraints on behavior
10. A generic safety control structure
11. The basic building block for a safety control structure
12. The Shell Moerdijk explosion
13. Very high-level safety control structure model for Shell Moerdijk
14. Shell Moerdijk safety control structure with more detail
15. Shell Moerdijk Chemical Plant safety control structure
16. Communication links theoretically in place in the Überlingen accident
17. The operational communication links at the time of the accident
18. The Lexington ComAir wrong runway accident safety control structure
19. Shein's model of organizational culture
20. The original, designed control structure to control water quality in Ontario, Canada
21. The control structure that existed at the time of the water contamination events.
22. The pharmaceutical safety control structure in the U.S.

B.1: Unit 4600 during normal production

B.2: Flawed interactions in the assumed safety control structure

C.1: Two designs of an error-prone stove top.

C.2: Less error-prone designs.

E.1: The abstraction System A may be viewed as composed of three subsystems. Each subsystem is itself a system.

E.2: System A can be viewed as a component (subsystem) of a larger system AB

E.3: The basic system engineering "V" model

# 그림 목차

그림1. 근본 원인 유혹은 아무것도 해결할 수 없음 ····· 12
그림2. 두더지 게임하기 ····· 13
그림3. 사후 확신 편향의 그래픽적 묘사 ····· 14
그림4. 다음 절차 딜레마 ····· 17
그림5. 사고 설명에 대한 두 가지 상반된 관점 ····· 20
그림6. 하인리히(Heinrich)의 도미노 모델 ····· 24
그림7. 리즌(Reason)의 스위스 치즈 모델 ····· 24
그림8. 시스템 이론에서의 발현 속성 ····· 28
그림9. 컨트롤러가 동작에 제약사항 강제 ····· 29
그림10. 일반적인 안전 컨트롤 스트럭처 ····· 30
그림11. 안전 컨트롤 스트럭처의 기본 빌딩 블록 ····· 31
그림12. 쉘 뫼르딕 플랜트 폭발 ····· 36
그림13. 쉘 뫼르딕 플랜트에 대한 매우 상위 수준의 안전 컨트롤 스트럭처 모델 ····· 48
그림14. 보다 상세한 쉘 뫼르딕(Shell Moerdijk) 안전 컨트롤 스트럭처 ····· 50
그림15. 쉘 뫼르딕 화학 플랜트의 안전 컨트롤 스트럭처 ····· 60
그림16. 위버링겐(Überlingen) 사고에서의 이론적 의사소통 링크 ····· 78
그림17. 사고 당시의 작업 의사소통 링크 ····· 79
그림18. 렉싱턴 공항에서의 컴에어 항공의 잘못된 활주로 사고에 대한 안전 컨트롤 스트럭처 ····· 80
그림19. 샤인(Shein)의 조직 문화 모델 ····· 84
그림20. 캐나다 온타리오주의 수질 컨트롤을 위해 설계된 컨트롤 스트럭처 원본 ····· 96
그림21. 수질 오염 이벤트 당시의 컨트롤 스트럭처 ····· 97
그림22. 미국의 제약(phamaceutical) 안전 컨트롤 스트럭처 ····· 106
그림B.1: 정상 생산 과정의 Unit 4800 ····· 122
그림B.2: 안전 컨트롤 스트럭처에서 결함이 있는 상호작용 ····· 124
그림C.1: 오류가 발생하기 쉬운 두 가지 스토브 상단 설계 ····· 134
그림C.2: 오류가 자주 발생하지 않는 설계 ····· 135
그림E.1: 세 개의 서브시스템으로 구성된 추상화 시스템 A. 각 서브시스템 자체가 하나의 시스템임 ····· 141
그림E.2: 시스템 A는 더 큰 시스템 AB의 컴포넌트(서브시스템)로 볼 수 있음 ····· 142
그림E.3: 기본적인 시스템 엔지니어링 "V-모델" ····· 146

# Chapter 1: Introduction

My goal for this handbook is not to provide a cookbook step-by-step process that you can follow like a recipe. While that is often what people want, the truth is that the best results are not obtained this way. Instead, they are generated by providing ways for experts to think carefully and in depth about the cause of an accident. We need tools that are able to encourage broader and deeper thinking about causes than is usually done. In this way, it is my hope that we are able to learn more from events.

It is always possible to superficially investigate an accident and not learn much of anything from the effort. The same accidents then occur over and over and are followed each time by the same superficial analyses. The goal instead should be to invest the time and effort needed to learn enough from each accident so that losses are dramatically reduced and fewer investigations are required in the future.

## *Why do we need a new accident analysis tool?*

The bottom line is that we are learning less from losses and near misses than we could. There are many accident analysis tools that have been created, particularly by academics, but few have significantly reduced accidents in real systems or even been used widely. Most focus on new notations for documenting the same old things.

If you want an academic and philosophical treatment of the subject, I recommend my "learning from events" paper[1] and my book *Engineering a Safer World* [Leveson 2012]. Reading *Engineering a Safer World* will help you to more deeply understand the limitations of current accident analysis approaches and assumptions and the technical and philosophical underpinnings of CAST. But that is not the goal of this handbook.

Instead, the goal here is to provide a practical set of steps to help investigators and analysts improve accident reports. Accident investigations too often miss the most important causes of an accident, instead choosing to focus on only one or two factors, usually operator error. This oversimplification of causality results in repetitions of the same accident but with different people involved. Because the *symptoms* of each loss seem to differ, we fix those symptoms but not the common underlying causes. As a result, we get stuck in continual fire-fighting mode.

## *What you will learn*

This handbook will teach you how to get more useful results from accident investigation and analysis. While it may be necessary to spend more time on the first few accident analyses using this approach, most of the effort spent in modeling and analysis in your first use of CAST will be reused in subsequent investigations. Over a short time, the amount of effort should be significantly reduced with a net long term gain not only in a reduction in time spent investigating future accidents but also in a reduction of accidents and thus investigations. Experienced accident investigators have found that CAST allows them to work faster on the analysis as it creates the questions to ask early, preventing have to go back later.

Your long-term goal should be to increase the overall effectiveness of the controls used to prevent accidents. These controls are often embedded in a Safety Management System (SMS). Investigating accidents and applying the lessons learned is a critical part of any effective SMS. In turn, the current weaknesses in your SMS itself will be identified through a thorough accident/incident analysis process. Investing in this process provides an enormous return on investment. In contrast, superficial analysis of

[1] Nancy Leveson, Applying Systems Thinking to Analyze and Learn from Events, Safety Science, Vol. 49, Issue 1, Januagey 2010, pp. 55-64.

# 1장: 소개

본 핸드북의 목표는 요리책 레시피와 같이 단계별로 따라할 수 있는 절차를 제시해 주는 것이 아니다. 사람들은 대게 이런 것들을 원하지만, 사실 최상의 결과들은 이런 식으로 얻어지는 것이 아니며, 사고 원인에 대해 전문가들이 신중하고 깊이 있게 생각할 수 있는 방법을 제공함으로써 얻어진다. 우리는 사고 원인에 대해 더욱 폭넓고 깊이 있는 생각을 이끌어내는 도구가 필요하다. 이 방법을 통해 우리가 이벤트로부터 더 많은 것을 배울 수 있기를 바란다.

우리는 항상 표면적으로 사고를 조사하고 그 결과에서 그리 많은 것을 배우지 못한다. 매번 같은 사고가 일어나고 동일하게 표면적인 분석을 되풀이 할 뿐이다. 사고에서 충분히 배울 수 있는 시간과 에너지를 투자해 손실을 획기적으로 줄이고 향후 조사가 거의 필요하지 않게 해야 한다.

### *왜 새로운 사고 분석 도구가 필요한가?*

결론적으로 말하면 우리는 손실과 니어 미스(near miss) 상황으로부터 실제 배울 수 있는 것보다 충분히 배우지 못하고 있다. 많은 사고 분석 도구들, 특히, 학자들이 개발한 많은 도구들이 있지만 실제 시스템에서 사고를 크게 줄이거나 널리 사용되는 경우가 드물다. 대부분 동일한 예전 것들을 새로운 표기법으로 문서화 하는 데 초점을 맞춘다.

본 주제에 대해 학문적이고 철학적으로 이해하고 싶다면, 논문 "learning from events"[1]와 필자가 저술한 책 *Engineering a Safer World [Leveson 2012]*를 추천한다. *Engineering a Safer World*를 보면 현 사고 분석 접근법과 가정의 한계점, CAST의 기술적, 철학적인 토대를 깊이 이해하는데 많은 도움이 될 것이다. 그러나 이것이 본 핸드북의 목표는 아니다.

이 핸드북의 목표는 조사관과 분석가가 사고 보고서 개선에 도움을 주기 위한 실무적 단계를 제공하는 것이다. 사고 조사 과정에서 가장 중요한 사고 원인들을 누락하거나, 운영자 실수와 같은 한 두 가지 원인에만 집중하는 경우가 많다. 원인에 대한 이러한 지나친 단순화는 개입된 사람들만 다를 뿐 사실상 같은 사고가 계속 반복되는 결과를 낳는다. 계속된 사고에서 손실의 *증상*이 다르므로 이러한 증상들을 해결하지만 공통적인 근본 원인들은 해결되지 않는다. 결과적으로 우리는 계속해서 fire-fighting 모드(역주: 눈앞의 현안을 해결하기에 급급한 상황)에 빠지게 된다.

### *무엇을 배울 것인가*

이 핸드북은 사고를 조사하고 분석할 때 더 유용한 결과를 얻는 법을 가르쳐 줄 것이다. 이 같은 접근법을 활용하면 처음 몇 번은 사고 분석에 더 많은 시간을 할애해야 할 수도 있다. 하지만 CAST를 처음 활용할 때 많은 노력을 들여 수행한 모델링 및 분석 결과들은 이후 사고조사에서 다시 활용될 것이다. 장기적 순 이익 관점에서, 향후 사고 조사에 소요되는 시간의 감소뿐만 아니라 사고의 감소와 그로 인한 조사 자체의 감소를 위한 노력의 양을 빠른 시일 내에 대폭 감소할 수 있도록 해야 한다. 경험이 있는 사고 조사관들은 CAST를 활용하면 질의해야 할 사항들을 조기에 확보하여 이후에 다시 이전 조사과정으로 되돌아가지 않아, 사고 분석을 더 빠르게 할 수 있다는 것을 알게 되었다.

사고를 예방하기 위해 필요한 컨트롤들의 효과를 전반적으로 높이는 것을 장기적인 목표로 삼아야 한다. 이러한 컨트롤은 안전 관리 시스템(SMS, Safety Management System)에 내포되는 경우가 많다. 사고 조사를 통해 얻은 교훈들을 반영하는 것은 효과적인 안전 관리 시스템의 중요한 부분이다. 결국 SMS가 가진 현재의 취약점들은 철저한 사고/사건 분석 절차를 통해 파악될 것이다. 이러한 분석 절차

[1] Nancy Leveson, Applying Systems Thinking to Analyze and Learn from Events, Safety Science, Vol. 49, Issue 1, Januagey 2010, pp. 55-64

why accidents are occurring in your organization or industry will primarily be a waste of resources and have little impact on future events.

In fact, the systemic causes of accidents even in diverse industries tend to be remarkably similar. In my career, I have been involved in the investigation and causal analysis of accidents in aviation, oil and gas production, space, and other fields as well as studying hundreds of accident reports in these and in most every other industry. The basic causal factors are remarkably similar across accidents and even industries although the symptoms may be very different. The types of omissions and oversimplifications in accident reports also tend to be very similar. That's actually good news because it means that there are lots of opportunities to improve learning from the past if we have the desire and the tools to do so. Sharing the results from CAST analyses that identify common systemic causes of losses will allow us to learn from others without having to suffer losses ourselves.

The STPA Handbook [Leveson and Thomas, 2018] teaches how to prevent accidents before they occur, including how to create an effective safety management system. But there are still likely to be accidents or at least near misses that occur, and sophisticated and comprehensive accident/incident analysis is an important component of any loss prevention program. With the exception of the U.S. Nuclear Navy program called SUBSAFE (described in Chapter 14 of *Engineering a Safer World*), no safety programs have eliminated all accidents for a significant amount of time. SUBSAFE has some unique features in that it severely limits the types of hazards considered (i.e., submarine hull damage leading to inability to surface and return to port), operates in a restricted and tightly controlled domain, and spends significant amounts of resources and effort in preventing backsliding and other factors that increase risk over time.

But even if one creates a perfect loss prevention program, the world is continually changing. While some changes are intentional and can be controlled, others are unplanned—systems themselves change over time, people's behavior within a system changes, and the environment within which the system operates will also change. Detecting the unsafe changes, hopefully by examining leading indicators of increasing risk (see Chapter 6 of the STPA Handbook) and thoroughly investigating near-misses and incidents using CAST, will allow unplanned changes to be identified and addressed before losses result.

There is no set notation or format provided in this handbook that must be used, although some suggestions are provided. The causes of different accidents may be best explained and understood in different ways. The content of the results, however, should not differ. The goal of this handbook is to describe a process for thinking about causation that will lead to more comprehensive and useful results. Those applying these ideas can create formats to present the results that are most effective for their own goals and their industry.

### *What is CAST?*

The causal analysis approach taught in this handbook is called CAST (Causal Analysis based on System Theory). Like STPA [Leveson 2012, Leveson and Thomas 2018], the loss involved need not be loss of life or a typical safety or security incident. In fact, it can (and has been) used to understand the cause of any adverse or undesired event that leads to a loss that stakeholders wish to avoid in the future. Examples are financial loss, environmental pollution, mission loss, damage to company reputation, and basically any consequence that can justify the investment of resources to avoid. The lessons learned can be used to make changes that can prevent future losses from the same or similar causes.

Because the ultimate goal is to learn how to avoid losses in the future, the causes identified should not be reduced to an arbitrary "root cause." Instead, the goal is to learn as much from every accident as possible. This goal is what CAST is designed to achieve. Some accident investigators have actually complained that CAST creates too much information about the causes of a loss. But, is a simple explanation your ultimate goal? Or should we instead be attempting to learn as much as possible from

를 활용하면 많은 이점이 있다. 반면에 조직이나 산업체에서의 사고 발생 원인을 피상적으로 분석하는 것은 자원을 낭비하는 것이며, 향후 사고 조사에 거의 도움을 주지 못할 것이다.

사실, 사고의 시스템적 원인(Systemic causes)은 다양한 산업 분야에 걸쳐 매우 유사한 경향을 띈다. 저자 본인은 항공, 석유 및 가스 생산, 우주 및 기타 분야에서 사고 조사와 원인 분석에 참여해 왔으며 대부분의 산업 분야에서 수백 건의 사고 보고서를 연구했다. 사고의 증상은 크게 다를 수 있지만, 기본적인 원인 요소(causal factors)는 사고와 산업 전반에 걸쳐 매우 유사하다. 사고 보고서의 누락 유형과 과도한 단순화 역시 매우 유사한 경향을 띈다. 한편으로 이런 경향은 긍정적인 부분도 있다. 만일 우리에게 수행 의지와 방법이 있다면 과거로부터 학습하여 개선할 여지가 많다는 것을 의미하기 때문이다. 손실을 야기하는 일반적인 시스템적 원인을 찾아낸 CAST 분석 결과를 공유하면 직접 손실을 겪지 않고도 타 사례로부터 배울 수 있다.

STPA 핸드북[Leveson and Thomas, 2018]을 통해 효과적인 안전 관리 시스템을 만드는 방법 뿐 아니라 사고 발생 전에 사고를 예방하는 방법을 알 수 있다. 그러나 여전히 사고 또는 최소한의 니어 미스가 발생할 가능성이 있기 때문에 정교하고 포괄적인 사고/사건 분석은 손실 방지 프로그램에 있어 중요하다. SUBSAFE라는 U.S. Nuclear Navy program(*Engineering a Safer World* 14장 참고)을 제외하고, 어떠한 안전 프로그램도 상당 시간 동안 모든 사고를 제거하지 못했다. SUBSAFE는 고려되는 위험(hazards) 유형(예: 수면 및 항구로의 복귀를 불가하게 하는 잠수함 선체 손상)을 극도로 제한하고, 제한적이고 엄격하게 통제되는 도메인에서 운영되며, 시간에 따라 리스크를 증가시키는 퇴행(Backsliding)이나 다른 요소들을 예방하는 데 상당한 자원과 노력을 소요한다는 점에서 몇 가지 독특한 특징을 갖는다.

그러나 완벽한 손실 방지 프로그램을 만든다고 해도 세상은 끊임없이 변화하고 있다. 어떤 변화는 의도적이고 통제 가능하지만, 어떤 변화는 계획되지 않은 것이다. – 시스템 자체는 시간이 지남에 따라 변하고 시스템 내 사람들의 행동도 변화하며 시스템이 작동하는 환경 역시 변할 것이다. 리스크 증가의 주요 선행지표(STPA 핸드북 6장 참조)를 검토하고 CAST를 이용해 니어 미스와 사건을 철저히 조사하며 안전하지 않은(unsafe) 변경사항을 탐지함으로써 손실 발생 전에 미리 의도하지 않은 변경사항들을 식별하고 해결할 수 있을 것이다.

이 핸드북에서는 반드시 사용해야 하는 표기법이나 형식을 제시하지는 않으며, 몇 가지 사항만 제안한다. 사고 원인은 사고마다 각기 다른 방식으로 가장 잘 설명되고 이해될 수 있다. 그렇다고 그 결과들의 내용이 달라져서는 안 된다. 이 핸드북의 목적은 보다 포괄적이고 유용한 결과를 이끌어 내는 인과관계 분석을 위한 프로세스를 제시하는 것이다. 이러한 아이디어를 적용하면 각 목표와 산업에 맞게 가장 효과적으로 결과를 도출할 수 있는 형식을 만들어낼 수 있다.

### *CAST란 무엇인가?*

이 핸드북에서 설명하는 원인 분석 접근법을 CAST(Causal Analysis based on System Theory)라고 한다. STPA[Leveson 2012, Leveson 및 Thomas 2018]에서 언급한 바와 같이, 관련된 손실이 생명 손실이나 전형적인 안전 또는 보안 사건일 필요는 없다. 실제로 STPA는 이해당사자들이 피하고자 하는 부정적 또는 원치 않는 이벤트의 원인을 파악하는 데 사용될 수 있으며 사용되어 왔다. 예를 들어 재정적 손실, 환경오염, 임무 실패, 기업 이미지 실추 그리고 기본적으로 손실 회피를 위해 자원 투입이 필요한 모든 결과들이 해당한다. 교훈(Lesson learned)은 동일 혹은 유사한 원인으로 인한 향후 손실을 예방할 수 있는 변화들을 만드는 데 사용될 수 있다.

궁극적인 목표는 미래의 손실을 방지하는 방법을 학습하는 것이므로, 확인된 원인들을 임의적인 “근본 원인(root cause)”으로 축소하지 않아야 한다. 대신, 가능한 모든 사고로부터 많은 것을 배우는 것으로

every causal analysis? Learning one lesson at a time and continuing to suffer losses each time is not a reasonable course of action. Systemic factors are often omitted from accident reports, with the result that some of the most important and far reaching causes are ignored and never fixed. Saving time and money in investigating accidents by limiting or oversimplifying the causes identified is false economy. The concept of "root cause" and "probable cause" are common ways to find someone or something to blame and then get on with life and business—until the next accident. The overriding question is whether to pay now or pay later.

*Relationship Between CAST and STPA*

Hazard analysis has been described as "investigating an accident before it occurs." STPA (System Theoretic Process Analysis) is a hazard analysis tool based on the same powerful model of causality as CAST. In contrast to CAST, its proactive analysis can identify all potential scenarios that may lead to losses, not just the scenario that occurred. These potential scenarios produced by STPA can then be used to prevent accidents before they happen. CAST, in contrast, assists in identifying only the particular scenario that occurred. Although their purposes are different, they are obviously closely related. Because STPA can be used early in the concept development stage of an accident (before a design is created), it can be used to design safety and security into a system from the very beginning, greatly decreasing the cost of designing safe and secure systems: Finding potential safety and security flaws late in the design and implementation can significantly increase development costs. CAST analyses of past accidents can assist in the STPA process by identifying plausible scenarios that need to be eliminated or controlled to prevent further losses.

*Format and Use of this Handbook*

This handbook starts with a short explanation of why we are not learning as much from accidents as we could be. Then the goals and the process for performing a CAST analysis are described. A real example of a chemical plant explosion in the Netherlands is used throughout. The causal factors in this accident are similar to most accidents. Many other examples of CAST analyses can be found in *Engineering a Safer World* and on the PSAS website (http://psas.scripts.mit.edu). Appendix A provides links to CAST analyses in a wide variety of industries.

The worlds of engineering safety and workplace safety tend to be unnecessarily separated with respect to both the people involved and the approaches used to increase safety. In fact, this separation is unnecessary and is inhibiting improvement of workplace safety. A chapter is included in this handbook on how to apply CAST to workplace (personal) safety.

While CAST and structured accident analysis methods have been primarily proposed for and applied to accidents involving physical systems, CAST can very effectively be used on social system "accidents," which may entail major disruptions, loss of life, or financial system losses. Examples are shown in Chapter 5 for a pain management drug (Vioxx) that led to serious physical harm before being withdrawn from the market and for the Bears Stearns investment bank failure in the 2008 financial system meltdown.

In summary, while there are published examples of the use of CAST as well as philosophical treatises on the underlying foundation, there are presently no detailed explanations and hints about how to do a CAST analysis. The goal of this handbook is to fill that void.

CAST is based on fundamental engineering concepts. For readers who do not have an engineering background, Appendix E will provide the information necessary to understand this handbook and perform a CAST analysis.

목표로 삼아야 한다. CAST는 이 목표를 달성하기 위해 설계되었다. 일부 사고 조사관들은 사실 CAST가 손실 원인에 대해 너무 많은 정보를 만들어낸다고 불평해왔다. 그런데, 당신의 궁극적인 목표가 단순한 설명인가, 아니면 모든 원인 분석으로부터 가능한 한 많은 것을 배우는 것인가? 한 번에 한 가지 교훈을 배우고 매번 계속해서 손실을 겪는 것은 합리적인 행동이 아니다. 시스템적 요인이 종종 사고 보고서에서 누락되며 그 결과, 가장 중요하고 광범위한 영향을 미치는 일부 원인이 누락되어 전혀 해결되지 않는다. 식별된 원인을 축소하거나 과도하게 단순화하여 사고 조사에 시간과 돈을 절약하는 것은 잘못된 경제적 관념이다. "근본 원인"과 "가능한 원인"이라는 개념은 비난할 만한 누군가 혹은 무언가를 찾아 비난하고 다음 사고가 일어나기 전까지 다시 일상을 유지하는 식의 보편적인 방편이다. 이 시점에서의 가장 중요한 질문은 지금 대가를 치를 것인가, 아니면 나중에 치를 것인가이다.

### *CAST와 STPA의 관계*

위험분석은 "사고 발생 전에 사고를 조사하는 것"이라고 설명되어 왔다. STPA(System Theoretic Process Analysis)는 CAST와 동일한, 강력한 인과관계 모델을 기반으로 하는 위험 분석 도구이다. CAST와는 달리, STPA의 사전 분석에서는 발생한 시나리오뿐만 아니라 손실로 이어질 수 있는 모든 잠재적 시나리오를 식별할 수 있다. STPA를 통해 생성한 잠재적 시나리오는 사고 발생 전에 미리 사고를 예방하는 데 활용될 수 있다. 이와 반대로, CAST는 이미 발생한 특정 시나리오만을 식별하는 데 유용하다. 비록 이 둘의 목적은 다르지만 분명 밀접한 관련이 있다. STPA는 사고의 개념 개발 단계 초기에 사용할 수 있기 때문에(설계가 만들어지기 전에), 처음부터 안전과 보안을 시스템 설계에 반영하는 데 사용할 수 있으며, 안전과 보안이 보장된 시스템 설계에 드는 비용을 크게 줄일 수 있다: 설계와 구현 시 잠재적인 안전 결함과 보안 결함을 늦게 발견하면 개발 비용이 크게 증가할 수 있다. 과거 사고에 대한 CAST 분석은 추가적인 손실을 예방하기 위해 제거 또는 통제해야 하는 발생 가능한 시나리오들을 식별함으로써 STPA 프로세스를 지원할 수 있다.

### *이 핸드북의 구성과 활용*

본 핸드북은 우리가 사고로부터 충분히 많은 것을 배우지 못하는 이유를 간단히 설명하는 것으로 시작하여 CAST 분석의 목표와 수행 과정을 설명한다. 네덜란드에서 발생한 화학 플랜트 폭발의 실제 예가 핸드북 전반에 걸쳐 사용된다. 이 사고의 원인 요소 대부분의 사고와 비슷하다. CAST 분석의 다른 많은 예는 Engineering a Safer World와 PSAS 웹 사이트 (http://psas.scripts.mit.edu)에서 찾을 수 있다. 부록 A에는 다양한 산업에서 이루어진 CAST 분석의 링크를 제공한다.

안전 공학과 작업장 안전 분야는 관련자 및 안전 증진에 사용되는 접근 방식 모두의 측면에서 불필요하게 분리되는 경향이 있다. 사실 이러한 분리는 불필요하며 오히려 작업장의 안전성 향상을 저해한다. 본 핸드북에는 작업장(개인) 안전에 CAST를 적용하는 방법을 소개하는 챕터가 포함되어 있다.

그간 CAST나 구조화 된 사고 분석 방법은 주로 물리적 시스템과 관련된 사고에 제안되고 적용되었지만, 사실 CAST는 중대 혼란이나 생명 손실, 금융 시스템에 손실을 수반할 수 있는 사회적 "사고"에도 매우 효과적으로 활용될 수 있다. 그 예로 5장에서 통증 관리 약물(Vioxx)의 시장 공급이 중단되기 전까지 신체적으로 심각한 피해를 입혔던 사례와 2008년 금융 체계에서의 베어스 스턴스 투자은행(Bears Stearns investment)의 파산 사례를 소개한다.

요약하면, CAST 개념을 토대로 한 철학적 논문과 CAST를 적용한 예들이 발표되긴 했지만, 아직까지 CAST 분석 방법에 대한 상세한 설명과 힌트들에 대한 내용은 없었다. 이 핸드북의 목표는 이러한 공백을 채우는 것이다.

CAST는 기본적인 공학 개념을 기반으로 한다. 공학적 배경지식을 가지고 있지 않은 독자들을 위해 부록 E에서 본 핸드북을 이해하고 CAST 분석을 수행하는 데 필요한 정보를 제공한다.

# Chapter 2: Starting with some Basic Terminology

*"When I use a word," Humpty Dumpty said, in rather a scornful tone, "it means just what I choose it to mean—neither more nor less." "The question is," said Alice, "whether you can make **words** mean so many different things." "The question is," said Humpty Dumpty, "which is to be master—that's all."*

Lewis Carroll (Charles L. Dodgson), *Through the Looking-Glass,* first published in 1872.

While starting from definitions is a rather dull way to start talking about an important and quite exciting topic, communication is often inhibited by the different definitions of common words that have developed in different industries and groups. Never fear, though, only a few common terms are needed, and this chapter is quite short.

As Humpty Dumpty (actually Charles Dodgson) aptly put it, the definitions established here apply to the use of this handbook, but are not an attempt to change the world. There is just no way to communicate without a common vocabulary.

*Accident* (sometimes called a *Mishap)*: An undesired, unacceptable, and unplanned event that results in a loss. For short, simply a loss.

Undesirability and unacceptability must be determined by the system stakeholders. Because there may be many stakeholders, a loss event will be labeled an accident or mishap if it is undesirable or unacceptable to any of the stakeholders. Those who find the loss desirable and acceptable will not be interested in preventing it anyway so to them this book will be irrelevant.

Note that the definition is extremely general. Some industries and organizations define an accident much more narrowly. For example, an accident may be defined as only related to death of or injury to a human. Others may include loss of equipment or property. Most stop there. The definition above, however, can include any events that the stakeholders agree to include. For example, the loss may involve mission loss, environmental pollution, negative business impact (such as damage to reputation), product launch delays, legal entanglements, etc. The benefit of a very broad definition is that larger classes of problems can be tackled. The approach to accident analysis described in this book can be applied to analyzing the cause of any type of loss.

It is also important to notice that there is nothing in the definition that limits the events to be inadvertent. They may be intentional so safety and security are both included in the definition. As an example, consider a nuclear power plant where the events include a human operator or automated controller opening a valve under conditions where opening it leads to a loss. The loss is the same whether the action was intentional or unintentional, and CAST can be used to determine why it occurred.

Universal applicability of the accident definition above is derived from the basic concepts of system goals and system constraints. The system goals stem from the basic reason the system was created: such as producing chemicals, transporting passengers or cargo, waging warfare, curing disease, etc. The system constraints are defined to be the acceptable ways those goals can be achieved. For example, it is usually not acceptable to injure the passengers in a transportation system while moving them from place to place. Events that damage the company's reputation while achieving short term profits may also not be acceptable to the stakeholders.

To summarize:

*System Goals*: the reason the system was created in the first place

# 2장: 기본 용어부터 시작하기

*"내가 어떤 단어를 말할 땐", 험프티 덤프티가 다소 깔보는 어조로 말했다. "그 단어는 바로 내가 선택한 의미만 가지는 거야. 그 이상도 그 이하도 아냐." "만약 그렇다면 문제는," 앨리스가 대꾸했다. "아저씨가 단어로 하여금 매우 많은 서로 다른 것을 의미하게 할 수 있느냐는 거죠." "문제는," 험프티 덤프티가 말했다. "누가 주인인가 하는 거지. 그게 다야."*

루이스 캐롤(Lewis Carroll) (본명, 샤를 L. 돗슨(Charles L. Dodgson)),
이상한 나라의 앨리스(Through the Looking-Glass), 1872년 초판발행.

중요하고 꽤 흥미로운 주제에 대해 이야기를 시작할 때 정의부터 시작하는 것은 다소 따분한 방법이긴 하다. 하지만 서로 다른 산업과 조직에서 동일한 용어를 다르게 정의하여 사용하기 때문에 의사소통이 어려워지는 경우가 있다. 그러나 걱정할 필요는 없다. 몇 가지 공통된 용어만 알면 된다. 그래서 이 장은 내용은 매우 짧다.

험프티 덤프티(실제로는 저자인 샤를 돗슨)가 말했듯이, 여기서 정의한 용어들은 이 핸드북에서 사용하기 위한 것이며 세상에서 사용하는 정의를 바꾸려는 것은 아니다. 공통된 어휘 없이는 의사소통을 할 방법이 없다.

*사고*(때로는 *미스햅(Mishap)* 이라고도 함) : 의도하지 않은, 수용할 수 없는, 계획되지 않은 이벤트, 간단히 말하면 손실(loss)

의도하지 않은 것과 수용할 수 없다는 것은 시스템 이해관계자에 의해 결정되어야 한다. 많은 이해관계자 중 한명이라도 손실 이벤트를 의도하지 않았거나 수용할 수 없는 것으로 여기는 경우 사고 또는 미스햅으로 분류된다. 손실을 의도하였거나 수용 가능한 것이라고 여기는 사람들은 어쨌든 손실 방지에 관심이 없을 것이므로 그러한 사람들에게 이 핸드북은 무관할 것이다.

정의는 매우 일반적이라는 점에 유의해야 한다. 일부 산업이나 조직에서는 사고를 훨씬 더 협소한 의미로 정의한다. 예를 들어 사고를 사람의 죽음이나 부상과 관련된 것으로만 정의할 수도 있다. 또 다른 곳에서는 장비나 재산상 손실을 포함하기도 한다. 대부분은 거기까지이다. 그러나 사고에 대한 위의 정의에는 이해관계자들이 포함하기로 동의한 어떤 이벤트들도 포함시킬 수 있다. 가령, 임무 손실, 환경오염, 부정적인 사업 영향(명성 손상 등), 제품 출시 지연, 법적 분쟁 등이 손실에 포함될 수 있다. 광범위한 정의의 장점은 더 넓은 범위의 문제들을 해결할 수 있다는 것이다. 이 책에서 설명하는 사고 분석에 대한 접근 방식은 어떤 유형의 손실에 대한 원인 분석에도 적용할 수 있다.

또한 사고의 정의에 있어 중요한 점은 이벤트를 반드시 의도하지 않은 것으로만 제한하지 않는다는 것이다. 때론 의도된 이벤트도 존재하므로 안전과 보안 모두 정의 대상에 포함될 수 있다. 예를 들어 원자력 발전소에서 밸브 개방이 손실을 초래하는 상황에서 운영자 또는 자동 컨트롤러가 밸브를 개방하는 이벤트를 생각해보자. 행동이 의도적이든지 의도적이지 않든지 동일한 손실이 발생하며 CAST는 이러한 손실이 발생한 이유를 파악하는 데 사용될 수 있다.

위의 사고 정의에 대한 보편적 적용 가능성은 시스템 목표와 시스템 제약사항의 기본적인 개념에서 비롯된다. 시스템 목표는 시스템이 만들어진 기본적인 이유에서 기인한다: 화학 물질 생산, 승객이나 화물의 운송, 전쟁을 벌이는 것, 질병 치료 등. 시스템 제약사항은 이러한 목표를 달성할 수 있는 수용 가능한 방법으로 정의된다. 예를 들어 운송 시스템이 승객을 이동시키면서 부상을 입히는 것은 일반적으로 허용되지 않는다. 단기적인 이익을 달성하면서 회사의 평판을 손상시키는 이벤트들 역시 이해관

*System Constraints*: the ways that the goals can acceptably be achieved

Notice here that the constraints may conflict with the goals. An important first step in system engineering is to identify the goals and constraints and the acceptable tradeoffs to be used in decision making about system design and operation. Using these definitions, system reliability is clearly not synonymous with system safety or security. A system may reliably achieve its goals while at the same time be unsafe or insecure or vice versa. For example, a chemical plant may produce chemicals while at the same time release toxins that pollute the area around it and harm humans. These definitions also explain why reliability may, in some cases, conflict with safety. A statement that a system "failed" does not provide enough information to understand what occurred or what goals or constraints were violated.

Two more definitions are needed. One is straightforward while the other is a little more complicated. The first is the definition of an incident or near-miss.

> *Incident* or *Near-Miss*: An undesired, unacceptable, and unplanned event that does not result in a loss, but could have under different conditions or in a different environment.

The final term that needs to be defined and used in CAST is *hazard* or *vulnerability*. The former is used in safety while the latter in security but they basically mean the same thing. A vulnerability is defined as a flaw in a system that can leave it open to attack while, informally, a hazard is a state of the system that can lead to an accident or loss. More formally and carefully defined:

> *Hazard or vulnerability*: A system state or set of conditions that, together with specific environmental conditions, can lead to an accident or loss.

As an example, a hazard might be an aircraft without sufficient propulsion to keep it airborne or a chemical plant that is releasing chemicals into the environment. An accident is not inevitable in either case. The aircraft may still be on the ground or may be able to glide to a safe landing. The chemicals may be released at a time when no wind is present to blow them into a populated area, and they may simply dissipate into the atmosphere. In neither case has any loss occurred.[2]

A loss results from the combination of a hazardous system state and environmental state:




The introduction of the term "hazard" is important in engineering. The engineers or system designers and the system operators only have under their control the system itself and not the environment. Because the goal is to prevent hazards, that goal is achievable only if the occurrence of the hazard is under someone's control. When designing the chemical plant, the designer does not have any control over which way the wind is blowing when chemicals are released into the environment. The only thing they and the operators can do is to try to prevent the release itself through the design or operation of the system, in other words, by controlling the hazard or system state. An air traffic control system can control whether an aircraft enters a region with potentially dangerous weather conditions, but air traffic control has no control over whether the aircraft is hit by lightning if it does enter the region. The aircraft designers have control over whether protection against lightning strikes is included in the aircraft

[2] One might argue that chemicals have been wasted but that would have to be included in the definition of a loss for the chemical plant and thus the hazard would be the chemical plant being in a state where chemicals could be released and wasted.

계자들에 의해 받아들여지지 않을 것이다.

요약하면:

*시스템 목표*: 처음에 시스템이 만들어진 이유

*시스템 제약사항*: 목표를 합당하게 달성할 수 있는 방법

여기서 제약사항이 목표와 상충될 수 있다는 점에 유의해야 한다. 시스템 엔지니어링에서 중요한 첫 단계는 시스템 설계와 운영에 대한 의사 결정에 사용할 목표와 제약사항, 수용 가능한 절충안을 파악하는 것이다. 이러한 정의에 비춰보면 시스템 신뢰성은 시스템 안전성 또는 보안과 명확히 동일한 개념은 아니다. 시스템은 안정적으로 목표를 달성할 수 있지만 동시에 안전하지 않거나 보안이 보장되지 않을 수 있다. 또는 그 반대의 경우도 마찬가지다. 예를 들어, 화학 플랜트는 화학 물질을 생산하는 동시에 주변 지역을 오염시키고 사람에게 해로운 독소를 방출할 수 있다. 이러한 정의는 어떤 면에서 신뢰성이 안전성과 상충될 수 있는지 그 이유에 대해서도 설명한다. 단순히 시스템이 "실패"했다는 진술은 무슨 일이 있었는지, 어떤 목표나 제약사항이 위반되었는지 이해하기에 정보가 불충분하다.

두 가지 정의가 더 필요하다. 하나는 간단하고 또 다른 하나는 좀 더 복잡하다. 첫 번째는 사건(incident) 또는 니어-미스(near-miss)에 대한 정의다.

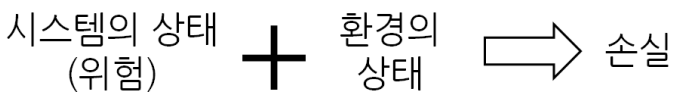
> *사건* 또는 *니어-미스* : 손실을 초래하지 않지만 다른 조건 또는 다른 환경에서는 손실이 발생할 수도 있는, 의도하지 않은, 수용할 수 없는, 계획되지 않은 이벤트

CAST에서 정의되어 사용되는 마지막 용어는 *위험(Hazard)* 또는 *취약성(vulnerability)*이다. 전자는 안전에 사용되고 후자는 보안에서 사용되는 용어이지만 기본적으로는 동일한 것을 의미한다. 취약성은 공격에 노출될 수 있는 시스템의 내부 결함으로서 정의되는 반면, 비공식적으로 위험은 사고나 손실로 이어질 수 있는 시스템의 상태를 의미한다. 보다 공식적으로 정의하면 다음과 같다:

> *위험 또는 취약성* : 특정한 환경 조건과 결합하여 사고나 손실을 유발할 수 있는 시스템 상태 또는 조건들의 집합

예를 들어 비행하기에 충분한 추진력이 없는 항공기 또는 화학물질을 주변 환경에 방출하는 화학 플랜트가 위험이 될 수 있다. 사고가 언제나 불가피하게 발생하는 것은 아니다. 항공기가 아직 지상에 있거나 활공하여 안전하게 착륙할 수도 있다. 인구가 밀집된 방향으로 바람이 불지 않을 때 화학물질이 방출될 수도 있으며 단순히 대기로 흩어질 수도 있다. 이러한 경우에는 손실이 발생하지 않는다.[2]

손실은 위험한 시스템의 상태와 환경의 상태의 조합으로 발생한다:




"위험"이라는 용어는 엔지니어링에서 중요한 의미를 가진다. 엔지니어 또는 시스템 설계자 그리고 시스템 운영자는 환경이 아니라 단지 시스템 자체에 대한 컨트롤만 가능하다. 위험을 예방하는 것이 목표이므로 위험의 발생여부가 누군가의 컨트롤 하에 있을 때만 목표가 달성될 수 있다. 화학 플랜트를 설계할 때, 설계자는 화학 물질이 대기에 방출될 때 바람이 부는 방향을 컨트롤 할 수 없다. 설계자

[2] 어떤 이는 이를 두고 화학물질이 헛되이 낭비된 것이라고 주장할 수 있다. 그렇다면 화학 플랜트에 대한 손실을 정의할 때 이 경우가 포함되어야 한다. 따라서 위험은 화학 플랜트가 화학물질을 방출할 수 있고 낭비할 수 있는 상태로 정의될 수 있다.

design, but not whether the aircraft will be struck by lightning. Therefore, when identifying system hazards, think about what things are under our control that could, in some particular environmental conditions, potentially lead to an accident. If no such environmental conditions are possible, then there is no hazard.[3]

Now let's go on to something that is hopefully more interesting.

[3] Some fields define "hazard" differently than system engineering. For example, in aviation, a mountain may be called a hazard because an airplane can be flown into it. But the goal in engineering is to eliminate or control a hazard. The mountain cannot, in most cases, be eliminated. The only thing the aircraft designers and operators have control over is staying clear of the mountain. Therefore, the hazard would be defined as violating minimum separation standards with dangerous terrain.

와 운영자가 할 수 있는 유일한 일은 시스템의 설계 또는 운영을 통해, 즉, 위험 또는 시스템 상태를 컨트롤하여 화학 물질의 방출 자체를 막는 것이다. 항공 교통 관제 시스템은 잠재적으로 위험한 기상 조건에 있는 지역에 항공기가 진입할지 여부를 컨트롤할 수는 있지만 항공기가 이 지역에 진입할 때 낙뢰 여부를 컨트롤 할 수는 없다. 항공기 설계자는 번개에 대비한 보호를 항공기 설계에 포함시킬지 여부를 컨트롤 할 수는 있지만 항공기가 번개를 맞을지를 컨트롤하지는 못한다. 그러므로 시스템 위험을 식별할 때에는 어떤 특정한 환경 조건에서 잠재적으로 사고로 이어질 수 있는, 우리의 컨트롤 하에 있는 것이 무엇인지를 생각해야 한다. 만약 그런 환경 조건이 존재하지 않다면 위험[3]도 존재하지 않는다.

이제 좀 더 흥미로운 내용으로 넘어가보자.

[3] 일부 분야는 “위험”을 시스템 엔지니어링과 다르게 정의한다. 예를 들어 비행 시 산은 위험이 될 수 있다. 항공기가 산으로 날아갈 수 있기 때문이다. 하지만 엔지니어링의 목표는 위험을 제거하거나 컨트롤 하는 것이다. 대개의 경우 산은 제거할 수 없다. 항공기 설계자와 운영자가 컨트롤 할 수 있는 유일한 것은 산에서 벗어나는 것이다. 따라서 위험은 위험 지형에 대한 최소 이격 거리 기준(minimum separation standards)을 위반하는 것으로 정의할 수 있다.

# Chapter 3: Why Aren't We Learning Enough from Accidents and Incidents?

*"A learning experience is one of those things that says, 'You know that thing you just did? Don't do that.'"*

Douglas Adams, *The Salmon of Doubt*, William Heinemann Ltd, 2001.

While there are many limitations in the way we usually do accident causal analysis and learn from events, five may be the most important: root cause seduction and oversimplification of causal explanations, hindsight bias, superficial treatment of human error, a focus on blame, and the use of models of causality that do not fit today's world.

## Root Cause Seduction and Oversimplification of Causality

Humans appear to have a psychological need to find a straightforward and single cause for a loss, or at least a very limited number of causes. John Carroll calls this "Root Cause Seduction." We want simple answers to complex problems. Not only does that make it easier to devise a response to a loss, but it provides a sense of control. If we can identify one cause or even a few that are easy to fix, then we can "solve the problem" and shift our attention to other concerns.

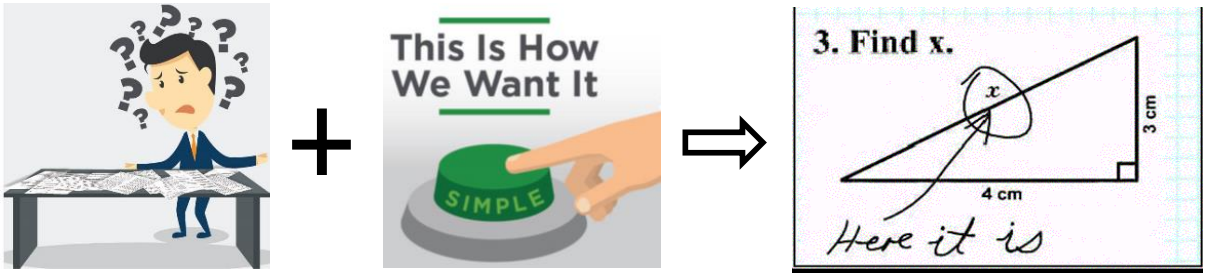



**Figure 1**: Root Cause Seduction leads nowhere.

The result of searching for a root cause and claiming success is that the problem is not fixed and further accidents occur. We end up in continual fire-fighting mode: fixing the symptoms of problems but not tacking the systemic causes and processes that allow those symptoms to occur. Too often we play a sophisticated "whack-a-mole" game and do not understand why the losses continue to occur. Enormous resources may be expended with little return on the investment.

# 3장: 사고와 사건으로부터 충분히 배우지 못하는 이유는 무엇인가?

*"학습 경험은 '방금 당신이 한 행동을 알고 있는가? 그렇게 하지 마라'라고 말하는 것이다"*

Douglas Adams, The Salmon of Doubt, William Heinemann Ltd, 2001.

우리가 일반적으로 사고 원인을 분석하고 이벤트로부터 학습하는 방식에는 많은 제약이 있겠지만, 그 중 다음의 다섯 가지가 가장 중요할 것이다: 근본 원인 유혹 및 원인 설명의 지나친 단순화①, 사후 확증 편향②, 인적 오류에 대한 표면적 논의③, 비난에 초점을 맞추는 것④, 오늘의 세계(현 시점)에 적합하지 않는 인과관계 모델을 사용하는 것⑤

## 근본 원인 유혹(seduction) 및 인과관계의 지나친 단순화①

사람은 심리적으로, 손실에 대해 간단하고 유일한 원인 또는 매우 제한된 수의 원인을 찾으려는 경향을 보인다. 존 캐롤(John Carroll)은 이것을 "근본 원인 유혹(root cause seduction)"이라고 부른다. 우리는 복잡한 문제에 대해 간단한 답을 원한다. 그것은 손실에 대한 대응을 쉽게 고안하도록 만들뿐만 아니라 컨트롤에 대한 감각을 제공한다. 해결하기 쉬운 원인을 하나 또는 몇 가지만 식별할 수 있다면 우리는 "그 문제를 해결"하고 다른 주제로 전환할 수 있다.

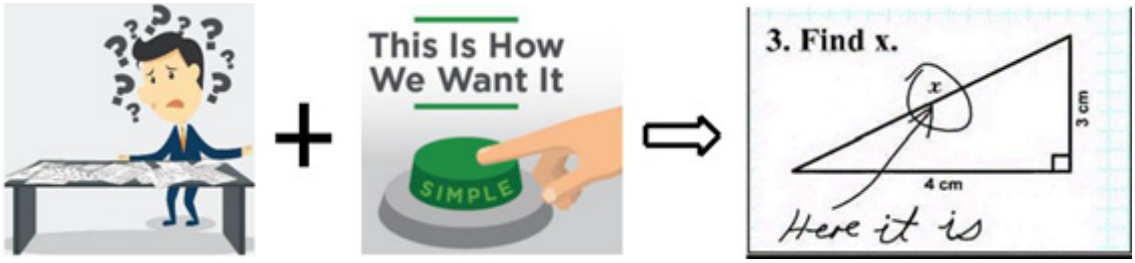



그림 1: 근본 원인 유혹은 아무것도 해결할 수 없음

근본 원인을 찾고 나서 성공했다고 주장하게 되면, 문제가 해결되지 않고 이후에 추가 사고가 발생하게 된다. 우리는 결국 계속되는 fire-fighting 모드(문제의 증상은 고치지만 그러한 증상이 발생할 수 있는 시스템적 원인과 프로세스를 고치지는 않는 것)에 빠지게 된다. 우리는 복잡한 "두더지" 게임을 너무 자주 반복하게 되며 손실이 계속되는 이유를 이해하지 못한다. 이는 낮은 ROI(Return On the Investment)와 함께 막대한 자원의 소비를 초래할 수 있다.



**Figure 2**: Playing Whack-a-Mole

Here are some examples of oversimplification of causal analysis leading to unnecessary accidents. In the crash of an American Airlines DC-10 at Chicago O'Hare Airport in 1979, the U.S. National Transportation Safety Board (NTSB) blamed only a "maintenance-induced crack" and not also a design error that allowed the slats to retract if the wing was punctured. Because of this omission, McDonnell Douglas was not required to change the design, leading to future accidents related to the same design error.

In the explosion of a chemical plant in Flixborough, Great Britain, in June 1974, a temporary pipe was used to replace a reactor that had been removed to repair a crack. The crack itself was the result of a poorly considered process modification. The bypass pipe was not properly designed (the only drawing was a sketch on the workshop floor) and was not properly supported (it rested on scaffolding). The jury-rigged bypass pipe broke, and the resulting explosion killed 28 people and destroyed the site. The accident investigators devoted much of their effort to determining which of two pipes was the first to rupture. The British Court of Inquiry concluded that "The disaster was caused by a coincidence of a number of unlikely errors in the design and installation of a modification" (the bypass pipe) and that "such a combination of errors is very unlikely ever to be repeated." [245].

Clearly, however, the pipe rupture was only a small part of the cause of this accident. A full explanation and prevention of future such losses required an understanding, for example, of the management practices of running the Flixborough plant without a qualified engineer on site and allowing unqualified personnel to make important engineering modifications without properly evaluating their safety, as well as storing large quantities of dangerous chemicals close to potentially hazardous areas of the plant and so on. The British Court of Inquiry investigating the accident amazingly concluded that "there were undoubtedly certain shortcomings in the day-to-day operations of safety procedures, but none had the least bearing on the disaster or its consequences and we do not take time with them." Fortunately, others ignored this overly narrow view, and Flixborough led to major changes in the way hazardous facilities were allowed to operate in Britain.

In many cases, the whack-a-mole approach leads to so many incidents occurring that they cannot all be investigated in depth, and only superficial analysis of a few are attempted. If instead, a few were investigated in depth and the systemic factors fixed, the number of incidents would decrease by orders of magnitude.

In some industries, a conclusion is reached when accidents keep happening that accidents are inevitable and that providing resources to prevent them is not a good investment. Like Sisyphus, they feel like they are rolling a large boulder up a hill with it inevitably crashing down to the bottom again until they finally give up, decide that their industry is just more dangerous than the others that have better accident statistics, and conclude that accidents are the price of productivity. Like those caught in any vicious circle, the solution lies in breaking the cycle, in this case by eliminating oversimplification of causal explanations and expanding the search for answers beyond looking for a few root causes.



그림 2: 두더지 게임하기

원인 분석의 지나친 단순화가 불필요한 사고로 이어진 몇 가지 사례를 소개한다. 1979년 시카고 오헤어(O'Hare) 공항에서 아메리칸 항공의 DC-10 항공기가 추락했는데 미국의 국가 교통 안전국(NTSB)에서는 그 원인으로 "유지 보수로 인한 균열"만 지적했으며 날개에 구멍이 났을 때 슬랫(slat, 역주: 항공기 날개 앞쪽에 있는 장치)을 접을 수 있도록 한 설계 오류는 지적하진 않았다. 이러한 누락으로 인해 맥도넬 더글라스(McDonnell Douglas)는 설계를 변경할 필요가 없었으며 이는 향후 동일한 설계 오류 관련 사고로 이어졌다.

1974년 6월, 영국 플릭스보로(Flixborough)에서 화학 플랜트 폭발 당시, 균열 수리를 위해 반응로(reactor)를 제거하고 임시 파이프로 대체하였다. 균열 자체는 공정 수정이 제대로 고려되지 않아서 발생한 결과였다. 바이패스 파이프는 제대로 설계되지 않았고(작업장 바닥에 스케치한 것이 유일한 도면이었음) 제대로 지지되지 않았다(비계(scaffolding) 위에 놓여 있었음). 결국 그 임시방편인 바이패스 파이프가 파손되고 반응로 폭발로 인해 28명이 사망했으며 현장이 붕괴되었다. 사고 조사관들은 두 개의 파이프 중 어느 것이 먼저 파열되었는지를 파악하기 위해 많은 노력을 기울였다. 영국 특별 조사 위원회(Court of Inquiry)는 "이번 재난은 수정사항을 설계 및 설치하는 과정에서 발생 가능성이 거의 없는 오류들이 우연히 동시 발생한 것이다"(바이패스 파이프)라고 하였고, "이런 오류의 조합이 반복될 가능성은 거의 없다"라고 결론 내렸다.

그러나 분명히 파이프 파열은 이 사고 원인의 작은 부분이었다. 충분한 설명과 향후 이런 손실의 예방을 위해서는 다음 관리 관행에 대한 이해가 필요하였다. 예를 들어 현장에 자격을 갖춘 엔지니어가 없는 상태에서 플릭스보로 플랜트를 운영하고, 자격이 없는 직원들이 안전을 제대로 평가하지 않고 중요한 엔지니어링을 수정하게 하는 것, 뿐만 아니라 플랜트의 잠재적 위험 지역 부근에 다량의 위험한 화학 물질을 보관하는 것 등이다. 사고를 조사하는 영국 특별 조사 위원회는 놀랍게도 "매일의 안전 절차 운영에는 의심할 여지없이 확실한 결점이 있었지만 그것들이 재난이나 그 결과에는 어떤 영향도 미치지 않았으므로 우리는 그러한 결점에 시간을 투자하지 않았다"고 결론 내렸다. 다행히 다른 사람들은 매우 편협한 이 의견을 무시했고 플릭스보로는 이후 영국에서 위험한 시설을 운영하는 방식에 큰 변화를 가져 왔다.

대부분의 경우, 두더지 게임 접근법은 많은 사건을 발생하게 하여 모든 사건을 심층적으로 조사할 수 없게 하였으며 일부 사건에 대해서는 표면적인 분석만 시도되었다. 만약 몇 개의 사건을 심도 있게 조사하고 시스템적 요인을 수정했다면 사건의 수는 수십 배 감소하였을 것이다.

일부 산업에서는, 사고가 계속 발생하는 경우, 불가피한 사고에 대해 사고 예방을 위해 자원을 제공하는 것이 좋은 투자가 아니라고 판단한다. 그들은 사고 예방을 위한 자원 제공이, 그리스 신화의 시

Accidents are always complex and multifactorial. Almost always there is some physical failure or physical equipment that had flaws in its design, operators who at the least did not prevent the loss or whose behavior may have contributed to the hazardous state, flawed management decision making, inadequate engineering development processes, safety culture problems, regulatory deficiencies, etc. Jerome Lederer, considered the Father of Aviation Safety, wrote:

> "Systems safety covers the total spectrum of risk management. It goes beyond the hardware and associated procedures of systems safety engineering. It involves: attitudes and motivation of designers and production people, employee/management rapport, the relation of industrial associations among themselves and with government, human factors in supervision and quality control, documentation on the interfaces of industrial and public safety with design and operations, the interest and attitude of top management, the effects of the legal system on accident investigations and exchange of information, the certification of critical workers, political considerations, resources, public sentiment and many other non-technical but vital influences on the attainment of an acceptable level of risk control. These non-technical aspects of system safety cannot be ignored."[4]

Our accident investigations need to potentially include all of these factors and more. This handbook will show you how.

## Hindsight Bias

A lot has been written about the concept of hindsight bias. At the risk of oversimplifying, hindsight bias means that after we know that an accident occurred and have some idea of why, it is psychologically impossible for people to understand how someone might not have predicted the events beforehand. After the fact, humans understand the causal connections and everything seems obvious. We have great difficulty in placing ourselves in the minds of those involved who have not had the benefit of seeing the consequences of their actions (see Figure 3).

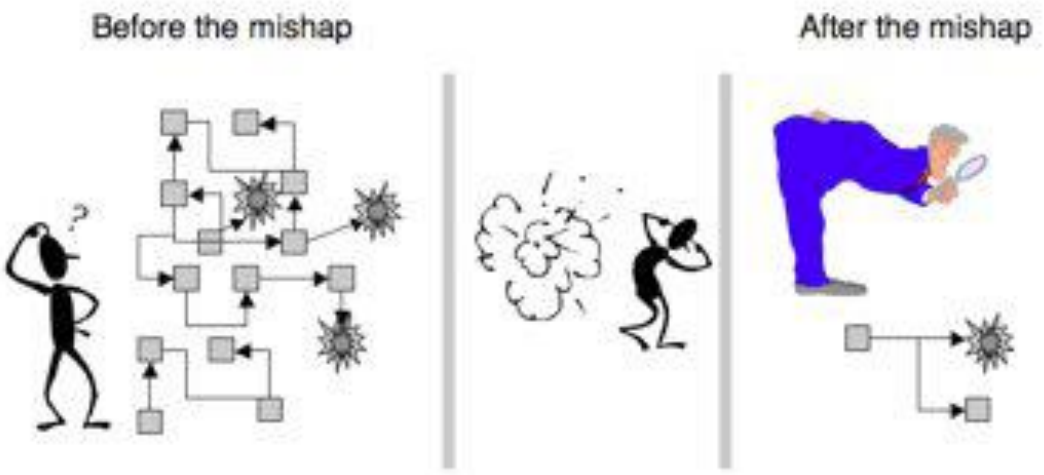



**Figure 3**: A graphical depiction of hindsight bias.
[Figure attributable to Richard Cook or Sidney Dekker]

Hindsight bias is usually found throughout accident reports. A glaring clue that hindsight bias is involved is when you see the words "he/she should have…," "he/she could have…," or "if only he/she

[4] Jerome Lederer, How far Have we come? A look back at the leading edge of system safety eighteen years ago, *Hazard Prevention*, page 8, May/June 1986.

시포스(Sisyphus)처럼, 필연적으로 바닥으로 다시 굴러 떨어질 커다란 바위를 포기하기 전까지 언덕 위로 굴리고 있는 것이라고 느끼고, 보다 좋은 사고 통계를 가진 다른 산업들보다 그들의 산업이 단지 조금 더 위험한 것이라 생각하며, 사고는 생산성의 대가라고 결론 내린다. 모든 악순환과 마찬가지로, 해결책은 사이클을 깨는 것에 있다. 이 경우에는 원인 설명에 대한 지나친 단순화를 없애고 몇 가지 근본 원인을 찾는 것 이상의 답을 찾는 것으로 확장하는 것이다.

사고는 항상 복잡하고 다원적(multifactorial)이다. 거의 대부분의 경우 물리적 고장, 설계에 결함이 있는 물리적 장치, 손실을 예방하지 않거나 위험 상태에 기여하는 운영자의 행동, 결함 있는 관리 의사결정, 부적절한 엔지니어링 개발 프로세스, 안전 문화 문제, 규제 결함 등의 문제가 있다. 항공 안전의 아버지로 여겨지는 제롬 레더러(Jerome Lederer)는 다음과 같이 말했다.

> "시스템 안전은 리스크 관리의 전체 스펙트럼을 커버한다. 그것은 하드웨어 및 시스템 안전 엔지니어링의 관련 절차를 초월한다. 설계자 및 생산자의 태도와 동기, 직원/관리자의 관계, 그들과 정부 사이의 산업 연대 관계, 감독 및 품질관리에서의 인적 요인, 설계와 운영관점에서 산업 및 공공 안전간의 인터페이스에 관한 문서, 최고 관리자의 관심과 태도, 법체계가 사고 조사와 정보 교환에 미치는 영향, 중요 작업자에 대한 인증, 정치적 고려사항, 자원, 대중의 정서 및 수용 가능한 리스크 컨트롤 수준 달성에 영향을 미치는 비기술적이지만 중요한 것 등을 의미한다. 시스템 안전의 이러한 비기술적인 측면은 무시해서는 안 된다."[4]

우리의 사고 조사에는 이러한 모든 요소들과 추가 요소들을 잠재적으로 포함시킬 필요가 있다. 이 핸드북에 그 방법이 소개되어 있다.

## 사후 확신 편향(Hindsight Bias)②

사후 확신 편향의 개념에 대한 많은 문헌들이 있다. 리스크의 지나친 단순화에서 사후 확신 편향은, 사고가 발생하고 그 발생 이유를 알게 된 후에는 사람들은 누군가가 이와 같은 사건을 미리 예측하지 못했다는 것을 심리적으로 이해할 수 없다는 것을 의미한다. 사람은 그 사실을 알고 나면 인과관계(causal connection) 및 모든 것이 명백하다고 이해한다. 우리는 어떤 행동의 결과를 미리 알 수 없는 입장에서 생각하는 데 큰 어려움을 겪는다(그림 3 참조).




그림 3: 사후 확신 편향의 그래픽적 묘사
[리차드 쿡(Richard Cook)과 시드니 데커(Sidney Dekker)의 그림 참조]

[4] Jerome Lederer, How far Have we com? A look back at the leading edge of system safety eighteen years ago, Hazard Prevention, page 8, May/June 1986.

would have …." Here are a couple of examples, one in a chemical plant and the other involving an aircraft.

After an accident involving the overflow of $SO^2$ (sulfur dioxide) in a chemical plant, the investigation report concluded that "*The Board Operator should have noticed the rising fluid levels in the tank*." [emphasis added] Sounds bad, right? Let's examine that conclusion.

The operator had turned off the control valve allowing fluid to flow into the tank, and a light came on saying it was closed. All the other clues that the operator had in the control room showed that the valve had closed, including the flow meter, which showed that no fluid was flowing. The high-level alarm in the tank did not sound because it had been broken for 18 months and was never fixed. There was no indication in the report about whether the operators knew that the alarm was not operational. Another alarm that was supposed to detect the presence of $SO^2$ in the air also did not sound until later.

One alarm did sound, but the operators did not trust it as it had been going off spuriously about once a month and had never in the past signaled anything that was actually a problem. They thought the alarm resulted simply from the liquid in the tank tickling the sensor. While the operators could have used a special tool in the process control system to investigate fluid levels over time (and thus determine that they were rising), it would have required a special effort to go to a page in the automated system to use the non-standard tool. There was no reason to do so (it was not standard practice) and there were, at the time, no clues that there was a problem. At the same time, an alarm that was potentially very serious went off in another part of the plant, which the operators investigated instead. As a result, the operators were identified in the accident report as the primary cause of the $SO^2$ release.

It's interesting that the report writers could not, even after careful study after the release, explain why the valve did not close and the flow meter showed no flow; in other words, why the tank was filling when it should not have been. But the operators were expected to have known this without any visible clues at the time and with competing demands on their attention. This is a classic example of the investigators succumbing to hindsight bias. The report writers knew, after the fact, that $SO^2$ had been released and assumed the operators should have somehow known too.

The words "should have" or their equivalent may not appear in the report, but hindsight bias may still be at work. As an example, one of the four probable causes cited in the accident report of the American Airlines B757 crash while approaching Cali, Columbia in 1995 was "*Failure of the flight crew to discontinue the approach into Cali, despite numerous cues alerting them of the inadvisability of continuing the approach*." In fact, the "cues" were only cues in hindsight if one already knows that a crash has occurred.

In summary, hindsight bias occurs because, after an accident, it is easy to see where people went wrong and what they should have done or avoided doing. It is also easy to judge about missing a piece of information that turns out to be critical only after the causal connections for the accident are made. It is almost impossible to go back and understand how the world looked to somebody not having knowledge of the later outcome.

How can hindsight bias be avoided, given that it is a natural result of 'after the fact" reasoning? It takes some effort and a change in the way we think about causality. Instead of spending our time focused on identifying what people did wrong when analyzing the cause of an accident, we instead need to start from the premise that the operators were not purposely trying to cause a loss but instead were trying to do the right thing. Learning can occur when we focus on identifying not what people did wrong

사후 확신 편향은 사고 보고서에서 일상적으로 발견된다. 사후 확신 편향이 개입된 명백한 단서는 "그/그녀가 했어야...", "그/그녀가 할 수 있었을지도..." 또는 "그/그녀만이 했었다면..."이라는 문구이다. 여기 두 가지 예제가 있다. 한 가지는 화학 플랜트이며 다른 한 가지는 항공기와 관련된 것이다.

화학 플랜트에서 $SO^2$(이산화황) 범람과 관련된 사고가 발생한 후 조사 보고서에서는 *"기판 운영자가 탱크 내 상승하는 유체의 높이를 알아챘어야 했다."*라고 결론 내린다. [강조 추가함] 잘못된 결론으로 보이지 않는가? 결론을 살펴보자.

운영자는 유체가 탱크로 유입되게 하는 컨트롤 밸브를 닫았고 밸브가 닫혔다는 표시등이 켜졌다. 운영자가 제어실에서 접할 수 있었던 모든 단서가 유량계와 밸브가 닫혀 있음을 보여 주었고 이는 유체가 흐르지 않고 있었음을 의미하였다. 탱크의 고수위(high-level) 경보음이 고장 나 있었지만 18개월간 고쳐지지 않았기 때문에 울리지 않았다. 보고서에는 운영자들이 경보음이 작동하지 않는다는 것을 알고 있는지에 대한 내용은 없었다. 공기 중에 $SO^2$가 있음을 탐지하는 또 다른 경보음도 나중까지도 울리지 않았다.

한 번의 경보음이 울렸지만, 경보음이 한 달에 한 번 정도 가짜로 울리고 있었고 과거에 실제 문제가 있을 때에도 울리지 않았기 때문에 운영자들은 경보음을 믿지 않았다. 그들은 탱크 안의 액체가 센서를 건드려서 경보음이 울린 것이라고 생각했다. 운영자가 공정 제어 시스템에서 특수 도구를 사용하여 시간에 따른 유체 레벨을 조사할 수 있었지만(따라서 상승 중이라고 판단할 수 있었음), 자동화 시스템에서 비표준(non-standard) 도구를 사용하는 페이지로 이동하려면 특별한 노력이 필요했을 것이다. (표준화된 관행이 아니었기 때문에) 그렇게 할 이유가 없었고 당시에는 문제가 있다는 단서가 없었다. 같은 시기에 공장의 다른 곳에서 매우 심각한 경보음이 울렸고 운영자는 그곳을 조사했다. 결과적으로 사고 보고서에서는 운영자가 $SO^2$ 유출의 주요 원인으로 식별되었다.

보고서 작성자가 유출 이후의 면밀한 연구에도 불구하고, 밸브가 닫히지 않고 유량계가 흐름이 없다고 표시한 이유를 설명할 수 없다는 것, 다시 말해 탱크가 채워져서는 안될 때 채워지는 이유를 설명할 수 없다는 점이 흥미롭다. 그러나 운영자들은 당시의 시각적 단서 없이도 지속적으로 관심을 가지고 이 사실을 알아내었어야 할 것으로 요구되었다. 이것은 조사관들의 사후 확신 편향에 대한 전형적인 예이다. 보고서 작성자들은 사후에 $SO^2$가 유출되었음을 알았고, 운영자들로 하여금 그 사실을 어떻게든 알았어야 한다고 생각했다.

보고서에 "했어야 함"이나 그에 상응하는 단어가 명시되지 않아도 사후 확신 편향은 여전히 있을 수 있다. 예를 들어 1995년에 콜롬비아 주(州) 칼리(Cali)에 접근하던 아메리칸 항공 B757기 추락사고 보고서에서 인용된 네 가지 가능한 원인 중 하나는 *"계속 접근하는 것이 부적절하다는 수차례의 알림 단서*(cues)*에도 불구하고 승무원이 칼리로 접근함"*이었다. 사실 "단서"는 충돌이 발생했다는 것을 이미 알고 있는 경우 사후 확증 단서일 뿐이었다.

요약하면, 사고가 난 후에는 사람들이 어디에서 잘못 되었는지, 무엇을 했어야 하는지, 무엇을 피했어야 하는지를 쉽게 알 수 있기 때문에 사후 확신 편향이 발생한다. 사고의 인과관계연결이 만들어진 후에만 중요한 것으로 판명되는 정보에 대해 그 누락을 판단하는 것은 쉽다. 나중의 결과를 모르는 사람의 관점으로 돌아가서 당시 상황이 어떻게 보였는지를 이해하는 것은 거의 불가능하다.

'사후' 추론의 자연스러운 결과라는 점을 감안할 때 사후 확신 편향은 어떻게 피할 수 있을까? 인과관계에 대한 우리의 사고방식에 약간의 노력과 변화가 필요하다. 사고 원인을 분석할 때 사람들이 무엇을 잘못했는지 파악하는 데 시간을 보내는 대신, 운영자들이 의도적으로 손실을 발생시키려 하지 않았고 올바른 일을 하려고 노력했다는 전제(premise)에서 출발해야 한다. 사람들이 잘못한 것을 파악하

but *why it made sense to them at the time to do what they did*.[5] CAST requires answering this type of question and leads to identifying more useful ways to prevent such behavior in the future.

## Unrealistic Views of Human Error

A treatise on human factors is not appropriate here. Many such books exist. But most accident analyses start from a belief that operator error is the cause of most incidents and accidents.[6] Therefore, it follows that the investigation should focus primarily on the operator. An assumption is made that the operator must be the cause and, unsurprisingly, the operator is then the focus of attention in the accident analysis and identified as the cause. Once the operator is implicated, the recommendations emphasize doing something about the operator (punish them, fire them, retrain the particular operator or all operators not to do the same thing again). The emphasis on human error as the cause of accidents is partly due to the "bad apple" theory, which arose a hundred years ago and was thoroughly discredited scientifically about seventy years ago. Unfortunately, it still persists. Appendix C provides more information about it. Heinrich also promulgated this theory around the same time.

Alternatively, or in addition, something may be done about operators in general. Their work may be more constrained by creating more rules and procedures—which may be impossible or unrealistic to expect them to always follow or which may themselves lead to an accident. Or the response may be to marginalize the operators by adding more automation. Adding more automation may introduce more types of errors by moving operators farther from the process they are controlling. Most important, by focusing on the operators, the accident investigation may ignore or downplay the systemic factors that led to the operator behavior and the accident.

As just one example, many accident investigations find that operators had prior knowledge of similar previous occurrences of the events but never reported them in the incident reporting system. In many cases, the operators did report them to the engineers who they thought would fix the problem, but the operators did not use the official incident-reporting system. A conclusion of the report then is that a cause of the accident was the operators not using the incident-reporting system, which leads to a recommendation to make new rules to enforce that operators always use it and perhaps recommend providing additional training in its use.

In most of these cases, however, there is no investigation of *why* the operators did not use the official reporting system. Often their behavior results from the system being hard to use, including requiring the operators to find a seldom-used and hard to locate website with a clunky interface. Reporting events in this way may take a lot of time. The operators never see any results or hear anything back and assume the reports are going into a black hole. It is not surprising then that they instead report the problem to people who they think can and will do something about it. Fixing the problems with the design of the reporting system will be much easier and more effective than simply emphasizing to operators that they have to use it.

A system's view of human error starts from the assumption that all behavior is affected by the context (system) in which it occurs. Therefore, the best way to change human behavior is to change the system in which it occurs. That involves examining the design of the equipment that the operator is using, carefully analyzing the usefulness and appropriateness of the procedures that operators are given

[5] For more about this, see Sidney Dekker, *The Field Guide to Understanding Human Error*, Ashgate Publishers, 2002.

[6] Much research is published that concludes that operators are the cause of 70-90% of accidents. The problem is that this research derives from looking at accident reports. Do the conclusions arise from the fact that operators actually are the primary cause of accidents or rather that they are usually blamed in the accident reports? Most likely, the latter is true. At best, such conclusions are not justified by simply looking at accident reports.

는 것이 아니라 *그들이 한 일이 그 당시 왜 타당하다고 생각되었는지를* 파악하는 데 집중할 때 우리는 배울 수 있다.[5] CAST에서는 이러한 유형의 질문에 대한 답을 요구하며 향후 이러한 행동을 예방할 수 있는 보다 유용한 방법을 찾을 수 있게 한다.

## 인적 오류에 대한 비현실적인 시각③

인적 요인에 관한 논문을 여기에 제시하는 것은 적절하지 않다. 관련 서적이 많이 있다. 대부분의 사고 분석은 운영자의 오류가 대부분의 사건과 사고의 원인이라는 믿음에서 시작된다.[6] 그러므로, 조사(investigation)의 초점을 주로 운영자에게 맞추려 한다. 운영자가 원인이 되어야 하고 운영자는 의심할 여지없이 사고 분석에서 주된 초점이며 원인으로 식별된다고 가정한다. 일단 운영자가 연루되면 권고사항에서는 운영자에 대한 조치를 강조한다(그들을 처벌하고 해고하며 특정 운영자 또는 모든 운영자가 같은 일을 반복하지 않도록 재교육한다). 사고 원인으로 인적 오류에 주안점을 두는 것은 부분적으로는 "썩은 사과(bad apple)" 이론에 기인한 것이다. 100년 전에 생겨난 이 이론은 약 70년 전에 전혀 비과학적인 것으로 확인되었지만 불행히도 여전히 지속되고 있다. 부록 C에서 그에 대한 더 많은 정보를 제시하고 있다. 하인리히(Heinrich) 또한 같은 시기에 이 이론을 널리 알렸다.

대안으로, 또는 추가로, 운영자에게 일반적으로 추가적인 무언가가 취해질 수 있다. 더 많은 규칙과 절차를 만들게 되면 그들의 업무가 더 제약받을 수 있다. 운영자들이 그러한 절차나 규칙을 항상 준수하는 것이 불가능하거나 비현실적이며 그것으로 인해 그들이 사고를 일으킬 수도 있다. 또는 더 많은 자동화를 추가하게 된다면 이는 운영자를 소외시키는 것일 수 있다. 자동화의 추가는 운영자들로 하여금 제어하고 있는 프로세스로부터 더 멀어지게 하여 더 많은 유형의 오류를 발생시킬 수 있다. 운영자에게 초점을 맞추었을 때 발생할 수 있는 가장 중요한 문제는, 사고 조사 과정에서 운영자 행동과 사고를 야기한 시스템적 요인을 무시하거나 경시할 수 있다는 것이다.

한 가지 예로 많은 사고 조사에서, 운영자가 이전에 유사 사건이 발생했던 것을 알고 있었음에도 사건 보고 시스템에 이를 알리지 않았다는 사실을 발견했다. 많은 경우에, 운영자는 문제를 해결할 것이라고 생각한 엔지니어에게 알릴뿐 공식 사건 보고 시스템을 사용하지는 않았다. 보고서의 결론에서는 사고의 원인을 사건 보고 시스템을 사용하지 않은 운영자로 보았고, 이는 운영자가 항상 따르도록 강제하는 새로운 규칙을 만들고 그 규칙에 대에 추가 교육할 것을 권장하는 것으로 이어졌다.

그러나 이런 경우의 대부분은, 왜 운영자가 공식 보고 시스템을 사용하지 않았는지에 대한 조사가 없다. 종종 이런 운영자들의 행동은, 인터페이스가 까다로워서 거의 사용하지 않거나 찾기 어려운 웹사이트를 찾아야 하는 등 시스템이 사용하기 어려울 때 발생한다. 이 방식으로 사건을 보고하는 것은 시간이 많이 걸릴 수 있다. 운영자는 시스템을 사용함에 따른 어떤 결과도 보거나 들을 수도 없었기에 시스템을 통해 작성한 보고서가 사라진다고 추측할 뿐이다. 그렇다면 그들이 문제에 대해 무언가를 할 수 있다고 생각하는 사람들에게 보고하는 것은 놀라운 일이 아니다. 단순히 운영자에게 보고 시스템을 사용해야 한다는 것을 강조하는 것보다 보고 시스템의 설계에 관한 문제를 해결하는 것이 훨씬 쉽고 효과적일 것이다.

인적 오류에 대한 시스템의 관점은 모든 행동은 발생하는 상황(시스템)에 영향을 받는다는 가정에

---

5 이에 대한 더 자세한 내용은 Sidney Dekker, The Field Guide to Understanding Human Error, Ashgate Publishers, 2002를 참조한다.

6 많은 연구에서 사고의 원인 중 70-90%가 운영자라고 결론 내렸다. 문제는 이러한 연구가 사고 보고서 검토에서 기인한다는 것이다. 운영자가 실제로 사고의 주요 원인이거나 일반적으로 사고 보고서에서 비난 받는다는 사실에서 결론이 도출되는가? 아마 후자는 그러할 것이다. 사고 보고서를 검토하는 것으로 그러한 결론이 정당화되는 것은 아니다.

to follow, identifying any goal conflicts and production pressures, evaluating the impact of the safety culture in the organization on the behavior, and so on.

Violating safety rules or procedures is interesting as it is commonly considered prima facie evidence of operator error as the cause of an accident. The investigation rarely goes into why the rules were violated. In fact, rules and procedures put operators and workers into an untenable situation where they are faced with a "following procedures" dilemma. Consider the model in Figure 4.

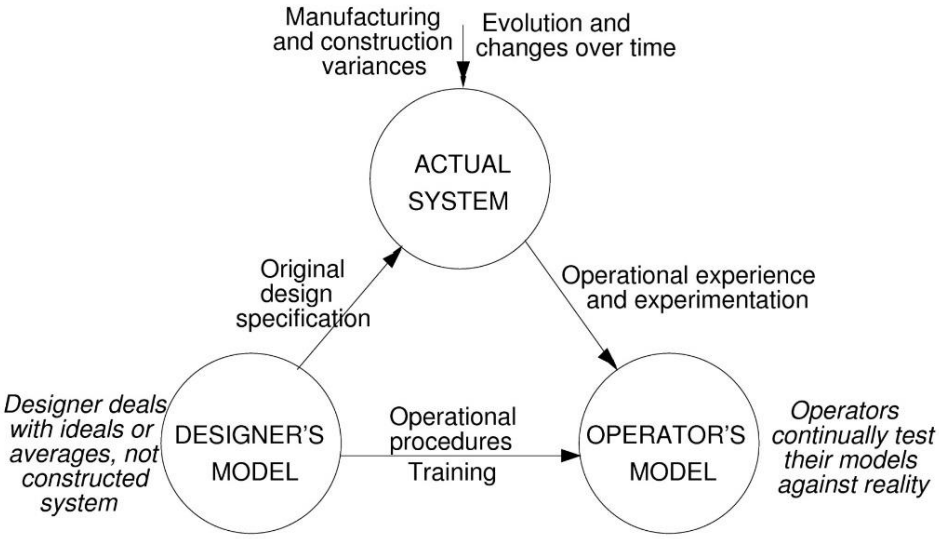



**Figure 4.** The Following Procedures Dilemma

There are always at least two mental models of the actual system: the designer's model and the operator's model. The designer provides or complies with the original design specification and the operational procedures and training guidance. The designer deals with ideals or averages (the ideal material or the average material) and assumes that the actual system will start out satisfying the original design specification and remain that way over time. The operational procedures and training are based on that assumption. In reality, however, there may be manufacturing and construction variances during the initial construction. In addition, the system will evolve and its environment will change over time.

The operator, in contrast, must deal with the actual system as it exists at any point in time, not the system that was originally in the designers' minds or in the original specifications. How do operators know what is the current state of the system? They use feedback and operational experience to determine this state and to uncover mistaken assumptions by designers. Often, operators will test their own mental models of the actual system state by performing "experiments" or informal tests. They are continually testing their own models of the system behavior and current state against reality.

The procedures provided to the operators by the system designers may not apply when the system behaves differently than the operators (and designers) expected. For example, the operators at Three Mile Island recognized that the plant was not behaving the way they expected it to behave. They could either continue to follow the utility-provided procedures or strike out on their own. They chose to follow the procedures, which after the fact were found to be wrong. The operators received much of the blame for the incident due to them following those procedures. In general, operators must choose between:

1. Sticking to procedures rigidly when cues suggest they should instead be adapted or modified, or
2. Adapting or altering procedures in the face of unanticipated conditions.

서부터 시작된다. 따라서 사람의 행동을 변화시키는 가장 좋은 방법은 그 행동이 발생하는 시스템을 변화시키는 것이다. 여기에는 운영자가 사용하고 있는 장비의 설계를 검토하고 운영자가 따르는 절차의 유용성과 적절성을 신중하게 분석하는 것이 포함된다. 또한 목표의 충돌과 생산에 대한 압박을 확인하고 조직 내 안전 문화가 행동에 미치는 영향을 평가하는 것 등도 포함된다.

안전 규칙이나 절차의 위반이 흥미로운 이유는 이러한 위반이 사고를 유발하는 운영자 오류의 일단 채택된 증거(prima facie evidence)로 간주되기 때문이다. 조사에서 규칙이 왜 위반됐는지는 거의 다루지 않는다. 사실, 규칙과 절차는 운영자와 작업자를 "다음 절차(following procedures)" 딜레마에 직면할 수밖에 없게 한다. 그림 4의 모델을 생각해보자.

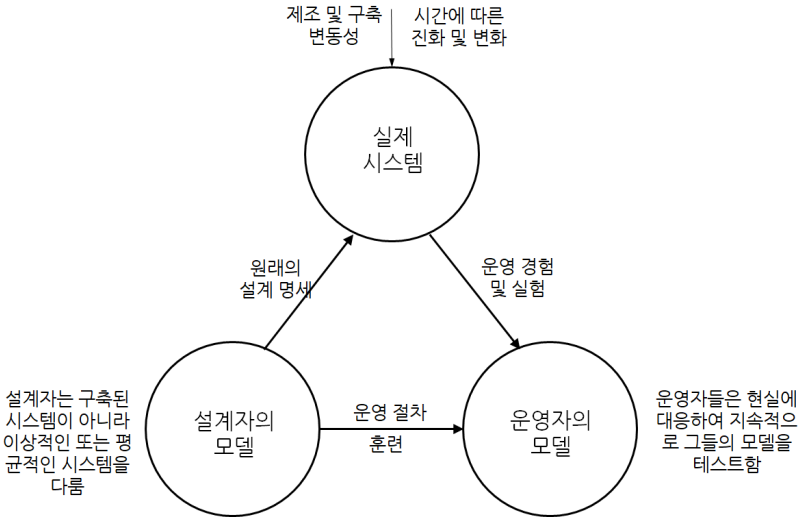



그림 4: 다음 절차(following procedure) 딜레마

실제 시스템에는 항상 적어도 두 가지 이상의 멘탈 모델이 있다: 설계자의 모델 및 운영자의 모델. 설계자는 원래의 설계 사양과 운영 절차 및 훈련 지침을 제공하거나 준수한다. 설계자는 이상적(ideals)이거나 일반적인 것(이상적인 재료 또는 보편적인 재료)을 다루며, 실제 시스템이 원래의 설계 명세를 충족하고 시간이 지나도 그대로 유지될 것이라고 가정한다. 운영 절차 및 훈련은 이러한 가정에 기초한다. 그러나 실제로는 초기 구축 과정에서 제조 및 구축의 변동성이 있을 수 있다. 또한 시스템은 진화할 것이고 그 환경은 시간이 지남에 따라 변할 것이다.

이와는 반대로 운영자는 원래 설계자의 생각에 있던 시스템 또는 원래의 명세에 있던 시스템이 아니라 특정 시점에 존재하는 실제 시스템을 다루어야 한다. 운영자는 시스템의 현재 상태를 어떻게 알 수 있을까? 그들은 피드백과 운영 경험을 활용하여 시스템의 상태를 결정하고 설계자의 잘못된 가정을 밝혀낸다. 종종 운영자는 "실험" 또는 비공식적인 테스트를 통해 실제 시스템 상태에 대한 그들 스스로의 멘탈 모델을 테스트한다. 그들은 시스템 동작과 현실에 대한 현재 상태에 대해 자신의 모델을 지속적으로 테스트한다.

시스템 설계자가 운영자에게 제공한 절차는 운영자(및 설계자)가 예상한 바와 시스템이 다르게 동작할 때에는 적용되지 않을 수 있다. 예를 들어, 쓰리마일 섬(Three Mile Island)의 운영자들은 발전소가 그들의 예상대로 동작하지 않고 있다는 것을 깨달았다. 그들은 사업자가 제시한 절차(utility-provided procedure)를 계속 따를 수도 있었고 자체적으로 판단할 수도 있었다. 그들은 절차를 따르기로 선택하였고 사후에 그 선택은 이후 잘못된 것으로 판명되었다. 운영자들은 그 절차를 따랐기 때문에 그 사건에 대한 많은 비난을 받았다. 일반적으로 운영자는 다음 중 하나를 선택해야 한다.

The first choice, following the procedures they were trained to follow, may lead to unsafe outcomes if the trained procedures are wrong for the situation at hand. They will be blamed for their inflexibility and applying rules without understanding the current state of the system and conditions that may not have been anticipated by the designers of the procedures. If they make the second choice, adapting or altering procedures, they may take actions that lead to accidents or incidents if they do not have complete knowledge of the current circumstances and system state and what might happen if they violate the written procedures. They will then be blamed for deviations and rule violations.

Following rules and procedures does not necessarily guarantee safety. Instead, safety comes from people being skilled in judging when and how to apply them. The traditional approach to safety contends that safety improvements come from organizations telling people to follow procedures, enforcing them, and assigning blame to people when accidents occur and there was a rule or procedure violation. In contrast, a system's approach to safety assumes that safety improvements come from organizations monitoring and understanding the gap between written procedures and practice (behavior) and updating procedures and rules accordingly. After accidents or incidents where written procedures or rules are violated, the focus should be placed on determining why the operators felt the need to disregard the procedures or rules. Simply concluding that the operators were at fault because they did not follow the written rules provides no useful information.

In general, the role of operators in modern systems is changing. Rather than directly controlling the system, humans are increasingly supervising automation, which is in fact implementing most of the detailed control tasks. At the same time, software is allowing enormously complex systems to be created, which are stretching the ability of people to understand them and leading to human behavior that under some conditions could be unsafe. In addition, systems are sometimes designed without using good human-centered and human-factors design principles. The result is that we are designing systems in which operator error is inevitable and then blaming accidents on operator error rather than designer error.

*Human error is a symptom, not a cause*. Consider another one of the four probable causes cited in the accident report for the American Airlines Cali accident: "Failure of the flight crew to revert to basic radio navigation at the time when the FMS-assisted navigation became confusing and demanded an excessive workload in a critical phase of flight." Notice that it is deemed to be the flight crew's fault for being confused and also for choosing to use poorly designed software (the FMS or Flight Management System) and not the fault of the software for being confusing and demanding an excessive workload. When accident reports state causes in this way, learning is inhibited and attention is directed to the wrong aspects of the causal scenario.

A systems approach to accident causation starts from the premise that human error is a symptom of a system that needs to be redesigned. Accident analysis should identify the design flaws and recommend ways they can be fixed, not blame the operators for the consequences of those design flaws.

## Blame is the Enemy of Safety

*Blame is a legal or moral concept, not an engineering one*

Focusing on blame seriously hinders what we learn from accidents. The goal of courts is to establish blame and liability. The goal of engineering, in contrast, is to understand *why* accidents occur so they can be prevented, not to establish blame and decide who was responsible.

A focus on blame in accident analysis has many unfortunate aspects that reduce learning from accidents and impedes preventing future ones. One result is that important information is often hidden: Those involved resort to pointing fingers at everyone else and searching for someone else to blame. The

1. 단서(cue)가 절차를 변경하거나 수정해야 하는 것으로 보이더라도 절차를 엄격히 고수함
2. 예상치 못한 상황에 직면하면 절차를 수정하거나 변경함

첫 번째 선택은, 즉, 준수하도록 교육받은 절차를 따르는 것은, 절차가 당면한 상황과 맞지 않으면 안전하지 않은 결과를 초래할 수 있다. 그들은 융통성 없음에 대해, 그리고 시스템의 현재 상태와 설계자들이 예상하지 못한 조건을 이해하지 않고 규칙을 적용한 것에 대해 비난받을 것이다. 만약 그들이 절차를 조정하거나 변경하는 두 번째를 선택한 경우, 그들이 현재 상황과 시스템 상태 그리고 서면 절차를 위반했을 때 발생할 수 있는 것에 대한 완전한 지식이 없다면, 이로 인해 사고나 사건이 발생할 수 있다. 그러면 그들은 일탈(deviation)과 규칙 위반에 대해 책임져야 할 것이다.

규칙과 절차를 따르는 것이 반드시 안전을 보장하는 것은 아니다. 대신 안전은 그것을 언제 어떻게 적용해야 하는지 판단할 수 있는 숙련된 사람들로부터 나온다. 안전에 대한 전통적인 접근 방식에서는, 사고가 발생하고 규칙이나 절차 위반이 발생하였을 때 사람들에게 절차를 따르고 강제하고 책임을 부여하도록 지시하는 조직에 의해 안전 개선이 비롯된다고 주장한다. 반대로, 안전에 대한 시스템적 접근법은 서면 절차와 관행(행동) 사이의 차이를 모니터링하고 이해하여 그에 따라 절차 및 규칙을 업데이트하는 조직에서 안전 개선이 비롯된다고 가정한다. 서면 절차나 규칙이 위반되는 사고 또는 사건이 발생한 이후에는 운영자가 절차나 규칙을 무시하게 된 이유를 파악하는 데 초점을 맞추어야 한다. 단순히 서면 규칙을 따르지 않았기 때문에 운영자가 잘못되었다고 결론 내리게 되면 유용한 정보를 얻을 수 없다.

일반적으로 최신 시스템에서 운영자의 역할은 변화하고 있다. 사람이 시스템을 직접 제어하기보다는 상세 제어 작업 대부분이 실제로 구현되는 자동화를 감독한다. 동시에 소프트웨어는 시스템을 매우 복잡하게 하여 사람들이 이해해야 하는 영역을 확장시키고 일부 조건에서는 사람으로 하여금 안전하지 않은 행동을 유발하게 한다. 또한 시스템은 때로는 우수한 사람 중심 및 인적 요인 설계 원칙 없이 설계된다. 그 결과, 운영자 오류가 불가피한 시스템을 설계한 다음 설계자 오류가 아닌 운영자 오류에 의한 사고로 책임을 전가시키고 있다.

*인적 오류는 원인이 아니라 증상이다.* American Airlines Cali 사고에 대한 사고 보고서에서 인용된 네 가지 가능한 원인 중 하나를 고려해보자: “비행의 중요 단계에서 FMS 보조 항법(FMS-assisted navigation) 장치에 혼동이 있고 동시에 과도한 작업량이 요구됨으로 인해 승무원이 기본 무선 항법(radio navigation)으로 복귀하지 못함”. 그것은 혼란스럽고 과도한 작업량을 요구한 소프트웨어의 오류로 간주되지 않고 혼동한 승무원 그리고 잘못 설계된 소프트웨어(FMS 또는 비행 관리 시스템)를 사용하기로 선택한 승무원의 잘못으로 간주된다. 사고 보고서에서 이런 식으로 원인을 서술하면 학습은 억제되고 관심은 원인 시나리오의 잘못된 측면으로 향하게 된다.

사고 원인에 대한 시스템 접근법은 인적 오류가 재설계 되어야 하는 시스템의 증상이라는 전제에서 시작된다. 사고 분석은 설계 결함의 결과에 대해 운영자를 비난하는 것이 아니라 설계 결함을 확인하고 그것을 수정할 수 있는 방법을 권고해야 한다.

## 비난(blame)은 안전의 적

*비난은 법적인 또는 도덕적인 개념이지 공학적인 것이 아니다*

비난에 초점을 맞추는 것은 사고로부터의 학습을 심각하게 방해한다. 조사 위원회(court)의 목표는 책임과 의무를 확고히 하는 것이다. 반면 공학의 목표는 사고가 왜 발생했는지를 이해하고 그것을 예방할 수 있는지를 검토하는 것이지, 비난받거나 책임질 사람을 결정하는 것이 아니다.

search for causes devolves to identifying the immediate actors in the event chain, usually the human operators or low-level managers, who obviously participated in the events and have no way to deflect attention onto others. The spotlight then is placed on the aspects of the loss that are least likely to provide important information about preventing future accidents.

C.O. Miller and Gerry Bruggink distinguished between an accusatory approach to causal analysis and an explanatory one. Here is a short exercise for the reader of this handbook. Consider the following conclusion from an accident report:[7]

*Exercise Part 1*. Description of the cause of the accident:

**WHO**

Accident Board **A** determined the probable cause of this accident was:

1. The flight crew's failure to use engine anti-icing during ground operations and takeoff.
2. Their decision to take off with snow/ice on the airfoil surfaces of the aircraft, and
3. The captain's failure to reject the takeoff during the early stage when his attention was called to anomalous engine instrument readings.

**WHY**

Contributing Factors:

1. The prolonged ground delay between de-icing and receipt of ATC clearance during which the airplane was exposed to continual precipitation
2. The known inherent pitch-up characteristics of the B-737 aircraft when the leading edge is contaminated with even small amounts of snow or ice, and
3. The limited experience of the flight crew in jet transport winter operations.

Using this description of the cause of the accident, where would you assign responsibility for this loss? What recommendations would you provide as a result? Are there additional questions you might ask during the investigation?

Discussion of your answer:

Did you assign responsibility to the flight crew? Why? What was the focus of the recommendations that you generated? Did they involve flight crew training and procedures? What other causal factors and recommendations did you generate? You might have mentioned something about the ground delay and avoiding that, but most likely all of your causes and recommendations involved the flight crew. That would not be surprising as their actions are identified in the analysis as the probable cause of the accident.

[7] Adapted from C.O. Miller, "Down with 'Probable Cause'!" International Society of Air Safety Investigators Seminar, Canberra, Australia, November 1991.

사고 분석에서 비난에 초점을 맞추는 것은 사고로부터의 배우는 것을 감소시키고 미래의 사고 예방을 방해하는 등 부적절한 측면이 많다. 그 중 한 가지 결과로, 중요한 정보가 숨겨질 때가 있다: 관련된 사람들은 다른 사람들을 지적하고 책임을 떠넘길 사람을 찾는 것에만 의존한다. 원인을 찾는 것은 이벤트 체인의 즉각적인 행위자를 식별하는 데 달려있는데, 일반적으로 명백히 이벤트에 관여하였고 다른 사람들에게 비난의 책임을 돌릴 수 없는 운영자 또는 낮은 수준의 관리자를 식별하는 것에 의존하게 된다. 그렇게 되면 미래의 사고 예방에 대한 중요한 정보를 제공할 가능성이 가장 적은 손실 측면이 주목받게 된다.

밀러(C.O. Miller)와 게리 브뤼긴크(Gerry Bruggink)는 원인 분석에 대한 비난적 접근과 설명적 접근을 구별하였다. 다음은 이 핸드북을 읽는 독자들을 위한 간단한 예제이다. 다음 사고 보고서[7]의 결론을 살펴보자.

*예제 Part 1*. 사고의 원인에 대한 설명 :

**누가(WHO)**

사고 위원회 **A**는 이 사고의 가능한 원인(probable cause)을 다음과 같이 결정하였다:

1. 승무원이 지상 운항과 이륙 과정에서 엔진 결빙 방지(anti-icing)를 사용하지 않음
2. 항공기의 에어포일 표면에 눈/얼음이 있는 상태로 이륙하기로 결정함
3. 기장이 초기 단계에서 비정상적인 엔진 계기 판독에 주의를 기울였기 때문에 이륙중지에 실패함

**왜(WHY)**

기여 요인:

1. 항공기가 지속적으로 강우(precipitation)에 노출되는 동안 제빙과 ATC 승인 수신 간의 오래 계속된 지상 지연(ground delay)
2. 리딩 엣지(leading edge)가 소량의 눈이나 얼음으로 오염되었을 때의 B-737 항공기 고유의 피치 업 특성
3. 승무원의 겨울철 제트 수송기 운항 경험 부족

사고의 원인에 대한 이 설명에 따른다면 손실에 대한 책임을 어디에 부여하겠는가? 결과적으로 어떤 권고사항을 내릴 것인가? 조사과정에서 추가 질문이 있는가?

당신의 답변에 대한 논의:

승무원에게 책임을 부여했는가? 왜 그랬는가? 당신이 만든 권고사항의 초점은 무엇인가? 그 권고사항에는 승무원 훈련 및 절차가 포함되었는가? 다른 어떤 원인 요소와 권고사항을 생성하였는가? 지상 지연과 그것을 회피하는 것에 대해 언급했을 수도 있지만 아마도 당신의 모든 원인과 권고사항은 승무원과 관련 있을 것이다. 분석 과정에서 그들의 행동이 사고의 가능한 원인으로 식별되기 때문에 놀랄 일은 아니다.

[7] 밀러(C.O. Miller)의 "Down with 'Probable Cause'!"에서 인용, International Society of Air Safety Investigators Seminar, Canberra, Australia, November 1991.

*Exercise Part 2*: Now consider a second description of the cause for the same accident:

**WHAT**

Based on the available evidence, Accident Board **B** concluded that a thrust deficiency in both engines, in combination with contaminated wings, critically reduced the aircraft's takeoff performance, resulting in a collision with obstacles in the flight path shortly after liftoff.

**WHY**

Reasons for the thrust deficiency:

1. Engine anti-icing was not used during takeoff and was not required to be used based on the criteria for "wet snow" in the aircraft's operations manual.
2. The engine inlet probes became clogged with ice, resulting in false-high thrust readings.
3. One crew member became aware of anomalies in cockpit indications but did not associate these with engine inlet probe icing.
4. Despite previous incidents involving false thrust readings during winter operations, the regulator and the industry had not effectively addressed the consequences of blocked engine inlet probes.

Reasons for the wing contamination:

1. Deicing/anti-icing procedures.
2. The crew's use of techniques that were contrary to flight manual guidance and aggravated the contamination of the wings.
3. ATC procedures that resulted in a 49-minute delay between departure from the gate and takeoff clearance.

Now, to whom or what would you assign responsibility for this accident? Was your list larger and different than the list you generated in exercise 1? Are there additional questions that you might like to investigate? Do you now think the cause was more than just "flight crew failures"? Did you identify other factors? What recommendations would you create from this analysis? How do the recommendations you generated differ from those for Exercise 1? Why? Did you generate design recommendations or recommendations involving groups or people other than the flight crew?

The first description of the accident (in Exercise 1) was *accusatory*. It focuses on the operators and their role in the loss, that is, on who was responsible. The second description (in Exercise 2) was *explanatory*. It does not focus on who but instead on what and why. Very different recommendations will result from each of these, although they are describing the same accident. We will learn more and find more causal factors if we use an explanatory approach rather than an accusatory one, that is, if we focus on what and why and not who.

| **Accusatory**: | **vs.** | **Explanatory**: |
|---|---|---|
| Who | | What |
| Why | | Why |

**Figure 5**: Two opposing views of accident explanation

*예제 Part 2.* 이제 같은 사고의 원인에 대한 두 번째 설명을 살펴보자:

**무엇(WHAT)**

사고 위원회 B는 가용한 증거를 바탕으로, 두 엔진의 추진력 부족이 오염된 날개 문제와 합쳐져 항공기의 이륙 성능을 심각하게 감소시켰으며 이륙 직후 비행 경로상의 장애물과 충돌하게 되었다고 결론 내렸다.

**왜(WHY)**

추진력 부족의 이유:

1. 이륙 중 엔진 결빙 방지 기능이 사용되지 않았으며 항공기 운영 매뉴얼의 "젖은 눈" 기준에 따라 사용할 필요가 없었음
2. 엔진 흡입구 프로브가 얼음으로 막혀서 추진력 수치가 잘못하여 높아짐
3. 한 승무원이 조종석 표시를 통해 이상 징후를 알았지만 이를 엔진 흡입구 프로브 결빙과 관련짓지 않음
4. 겨울철 운영 중 잘못된 추진력 판독과 관련된 과거의 사건이 있었음에도 불구하고 규제 기관과 산업계에서 엔진 흡입구 프로브가 막힌 것을 효과적으로 해결하지 못했음

날개 오염의 이유:

1. 제빙/결빙 방지 절차
2. 승무원이 비행 매뉴얼 지침에 위배되는 방법으로 날개의 오염을 악화시켰음
3. 게이트에서 출발한 시점부터 이륙 허가까지의 49분 지연을 초래한 ATC 절차

이제 이 사고에 대해 누구에게 또는 무엇을 책임지게 하겠는가? 당신이 작성한 목록은 1번 예제에서 작성한 목록보다 더 많고 다른가? 확인하고 싶은 추가 질문이 더 있는가? 그 원인이 단순히 "승무원의 실패" 그 이상의 것이라고 생각하는가? 다른 요인들도 식별했는가? 이 분석에서 어떤 권고사항을 제시할 것인가? 당신이 제시한 권고사항은 예제 1의 권고사항과 어떻게 다른가? 왜 다른가? 승무원 이외의 그룹이나 사람과 관련된 권고사항 또는 설계 권고사항을 작성하였는가?

사고에 대한 첫 번째 설명(예제 1)은 *비난적(accusatory)이었다.* 그 설명은 운영자 및 손실에 대한 그들의 역할, 즉 누구에게 책임이 있는지에 초점을 맞춘다. 두 번째 설명(예제 2)은 *설명적(explanatory)*이었다. 그 설명은 누구냐에 초점을 맞추는 것이 아니라 무엇인지와 왜인지에 초점을 맞추고 있다. 이들 각각은 매우 다른 권고사항을 도출할 것이다. 우리가 비난적인 접근법보다는 설명적인 접근법을 사용한다면, 즉, 누구(who)가 아니라 무엇(what)과 왜(why)에 초점을 맞춘다면 더 많은 것을 배우고 더 많은 원인 요소를 발견할 것이다.

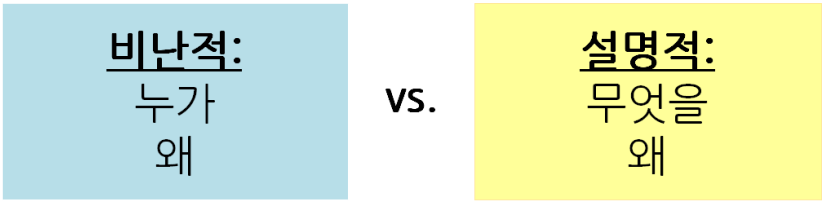



그림 5: 사고 설명에 대한 두 가지 상반된 관점

Another thing to notice in these two exercises is the use of the word "failure" in the first but not in the second. Failure is a pejorative word, that is, it involves judgement and assignment of blame. Consider the two following two statements, differing only in the use of the word "failure":

1. The captain's failure to reject the takeoff during the early stage when his attention was called to anomalous engine instrument readings.
2. The captain did not reject the takeoff during the early stage when his attention was diverted to anomalous engine instrument readings.

The first suggests a conclusion that the captain did something wrong. Further exploration is not encouraged because it is stated as a conclusion. A judgment has been made about the captain's actions. A cause has been determined, and that cause was a failure on the part of the captain. The second is a simple statement of what the captain did without any judgment in it. It encourages further exploration about why the captain's attention might have been drawn to the anomalous engine instrument readings and, even more important, why anomalous readings were produced.

Is this really a problem in accident reports? In fact, the conclusion of "failure" pervades most accident reports. Here is an example of the conclusions from an aircraft CFIT (Controlled Flight into Terrain) accident at Birmingham Shuttlesworth International Airport,[8] which is typical. The NTSB concluded that:

> "The probable cause of this accident was the flight crew's continuation of an unstabilized approach and their failure to monitor the aircraft's altitude during the approach, which led to an inadvertent descent below the minimum approach altitude and subsequently into terrain.

The report also concludes that contributing to the accident were:

(1) the flight crew's failure to properly configure and verify the flight management computer for the profile approach;
(2) the captain's failure to communicate his intentions to the first officer once it became apparent the vertical profile was not captured;
(3) the flight crew's expectation that they would break out of the clouds at 1,000 feet above ground level due to incomplete weather information;
(4) the first officer's failure to make the required minimums callouts;
(5) the captain's performance deficiencies likely due to factors including, but not limited to, fatigue, distraction, or confusion, consistent with performance deficiencies exhibited during training; and
(6) the first officer's fatigue due to acute sleep loss resulting from her ineffective off-duty time management and circadian factors.

[emphasis added]

Notice that the conclusions about the probable cause and contributing factors for this accident identify only flight crew behavior and the events that reflect flight crew "failures." *Why* the flight crew behaved the way they did is not included (except for fatigue, which does not fully explain it). One contributory factor does mention a reason, i.e., (3) the flight crew's expectation that they would break out of the clouds at 1,000 feet above ground level due to incomplete weather information. But the emphasis here is on the flight crew behavior and expectations and not why incomplete weather information was provided to the crew. The system design flaws related to providing weather and needing to be fixed are not mentioned in the accident causal summary.

[8] National Transportation Safety Board, Crash During a Nighttime Nonprecision Instrument Landing, UPS Flight 1354, Birmingham, Alabama, August 14, 2013, Accident Report NTSB/AAR-14/02, 2014.

이 두 가지 예제에서 주목해야 할 또 다른 사항은, 첫 번째 예제에서는 "실패"라는 단어를 사용하나 두 번째 예제에서는 사용하지 않는다는 것이다. 실패는 비방적인 단어, 즉, 책임의 판단과 할당을 내포한다. "실패"라는 단어의 사용만으로 차이가 나는 다음 두 가지 진술을 살펴보자.

1. 기장이 비정상적인 엔진 계기 판독에 주의를 기울인 초기 단계에서 이륙중지에 실패함
2. 기장이 비정상적인 엔진 계기 판독에 주의를 돌려 초기 단계에서 이륙중지를 하지 않았음

첫 번째는 기장이 뭔가 잘못했다는 결론을 내린다. 결론으로서 기술되기 때문에 추가적인 탐구가 수행되지 않는다. 기장의 행동에 대한 판단이 내려졌다. 원인이 밝혀졌는데 그 원인은 기장 측의 실패였다. 두 번째는 어떤 판단도 없는 기장이 무엇을 했는지에 대한 단순한 문장이다. 그 문장은 왜 기장의 주의가 비정상적인 엔진 계기 판독에 끌렸는지 그리고 더 중요한 것은 왜 비정상적인 판독이 발생되었는지에 대해 더 많이 탐구하게 한다.

사고 보고서에서 이것이 실제로 문제가 되는가? 실제로 "실패"의 결론은 대부분의 사고 보고서에 널리 퍼져 있다. 버밍엄 셔틀즈워스(Birmingham Shuttlesworth) 국제공항에서 발생한 항공기 CFIT(Controlled Flight into Terrain, 조종상태에서의 지형충돌) 사고[8]의 결론이 전형적인 예이다. 미국 연방 교통 안전 위원회(NTSB)는 다음과 같이 결론지었다.

> "이 사고의 가능한 원인은 승무원들이 불안정한 접근을 계속 시도하고 접근하는 동안 항공기의 고도 모니터를 실패한 것이고, 이로 인해 최소 접근 고도 이하로 의도치 않게 하강하게 되어 이후 지형과 충돌하였다."

이 보고서는 또한 사고에 기여한 것은 다음과 같다고 결론지었다.

(1) 승무원들이 프로파일 접근을 위한 비행관리 컴퓨터를 적절하게 구성 및 검증하는 데 실패함
(2) 수직 프로파일이 캡처되지 않은 것이 명백할 때 기장이 부기장에게 그의 의도 전달하는 것에 실패함
(3) 승무원이 불완전한 날씨 정보로 인해 지상 1000피트 상공에서 구름을 벗어날 것이라고 기대함
(4) 부기장이 요구되는 최소 콜아웃(callout)에 실패함
(5) 훈련 중 나타나는 역량 부족과 동일한, 피로, 산만함 또는 혼란 및 이외의 요인들로 인한 기장의 역량 부족
(6) 비효율적인 근무 외 시간 관리 및 24시간 주기의 생체 리듬(circadian) 요인에서 비롯된 심각한 수면 부족으로 인한 부기장의 피로감

[강조 추가함]

이 사고의 가능한 원인 및 기여 요인에 대한 결론은 승무원의 행동과, 승무원의 "실패"를 반영하는 이벤트만을 식별한다는 점에 유의해야 한다. 승무원이 그렇게 행동한 이유는 포함되지 않는다(피로를 제외하고는 완전히 설명되지 않는다). 한 가지 기여 요인에 대한 이유로, (3) 승무원이 불완전한 날씨 정보로 인해 지상 1,000피트의 구름에서 벗어날 것이라는 기대를 언급하기는 한다. 그러나 여기서 강조하는 것은 승무원의 행동과 기대이며 왜 불완전한 날씨 정보가 승무원에게 제공되었는지에 대한 것이 아니다. 날씨 정보 제공과 관련되어 있으며 고쳐져야 할 시스템 설계의 결함은 사고 원인 요약에 언급되어 있지 않다.

---

8 미국 연방 교통 안전 위원회(NTSB, National Transportation Safety Board), 야간 정밀 장비 착륙 과정에서의 충돌, UPS 비행 1354, 버밍엄, 알라바마, 8월 14일, 2013년, 사고 보고서 NTSB/AAR-14/02, 2014.

Alternatively, a systems approach using CAST would not only look at what the pilots did that contributed to the accident but, more important, *why* they believed it was the right thing to do at that time.[9] The official conclusions omit most of the information that would be useful in preventing such accidents in the future. We don't learn why the flight crew behaved the way they did because the explanation stops with the conclusion that they "failed." In addition, the entire system for preventing CFIT (which has been a focus of accident prevention for many years) needs to be examined—not just the pilot behavior. Some of the many contributors to this accident were the design of the automation, landing on a runway without an instrument landing system, lack of an air traffic control alert to indicate that the aircraft was too low, maintenance practices at the airport, the ground proximity warning system not providing an alert until too late (due in part to the airline not upgrading the warning system with the new software provided), and a dozen other factors that are more likely to lead to useful recommendations than simply identifying the "failures" of the flight crew.

The use of the word "failure" pervades the causal description of most accident reports. It is erroneously applied not only to humans but to software, operators, and management decision making.

Software does not "fail"; it simply executes the logic that was written. There needs to be an examination of why unsafe software was created—usually it can be traced to requirements flaws—and recommendations involving improvement of the process that produced the unsafe software. Concluding that the "software failed" makes no technical sense and provides no useful information.

Humans also do not "fail" (unless their heart stops). They simply react to the situations in which they find themselves. What they did may, in hindsight, turn out to have been the wrong thing to do. But why it seemed to them to be the right thing at the time needs to examined in order to make useful recommendations. Again, simply recounting what people did wrong provides no useful information beyond creating a convenient scapegoat for the accident. Understanding why they behaved the way they did will focus the accident analysis in a useful direction.

And finally, companies do not fail unless they go out of business. A typical example found in accident reports is a statement that "Company X failed to learn from prior events." Companies are pieces of paper describing legal entities. Documents do not learn or, for that matter, fail. The company may be made up of hundreds, thousands, or even tens of thousands of employees. More useful would be to determine why learning did not take place and to ask questions such as: Is there a safety information system that captures prior adverse events so that learning can occur? If so, were the prior events recorded in the safety information system? If not, then why not? Were they just missed accidentally, was there no process to include them, or was the process not followed? If the latter, why was the process not followed? If the previous events were recorded, then why were they not used? Were they hard to find or was enough information not included to prevent repetition? Were there procedures in place to require using recorded information? And so on. Answering these questions will provide information useful for creating recommendations that will improve future learning from events and prevent repetition of the losses. Simply concluding that "the company failed to learn from events" only assigns blame without providing the information necessary to improve the situation in the future.

Eliminating the use of "failure" will greatly enhance learning from accidents. By not short-circuiting the search for understanding by concluding there was a "failure," we could immeasurably improve accident investigation and learning and, hopefully, safety.

More generally, to increase learning from losses, we need to eliminate the focus on assigning blame in accident reports. This may be hard to do: there seems to be a human need to find someone responsible for a tragedy. But a choice has to be made between personal satisfaction in identifying a villain or seizing the opportunity to prevent more such accidents in the future. Engineers should leave

[9] Sidney Dekker, *A Field Guide to Understanding Human Error*, London: Ashgate, 2006.

CAST를 활용한 시스템 접근 방식은 조종사들이 사고에 기여한 것들을 살펴보기도 하지만 그보다 중요하게는, 당시에[9] 그 행동이 *왜* 옳은 일이라고 믿었는지에 대한 것 또한 살펴본다. 공식적인 결론에서는 향후 그러한 사고를 예방하는 데 유용할 대부분의 정보를 담지 않는다. "실패함"이라는 결론으로 설명이 중단되기 때문에 승무원들이 왜 그렇게 행동했는지는 배우지 못한다. 게다가, 단지 조종사의 행동뿐만 아니라 (수년 동안 사고 예방의 초점이었던) CFIT 예방을 위해 시스템 전체를 점검해야 한다. 이 사고에 기여한 많은 요인 중에는 자동화 설계, 계기 착륙 시스템 없이 활주로에 착륙, 항공기가 너무 낮게 날고 있다는 것을 나타내는 항공 교통 관제 경보의 부족, 공항의 유지보수 관행, 지상 근접 경고 시스템이 너무 늦게까지 경보를 제공하지 않는 것(부분적으로는 항공사가 새로운 소프트웨어를 통해 경고 시스템을 업그레이드하지 않기 때문), 그리고 단순히 승무원의 "실패" 식별이 아닌 유용한 권고사항으로 이어질 수 있는 다른 수많은 요인이 있었다.

"실패"라는 단어는 대부분의 사고 보고서의 원인 설명에 만연해있다. 그 단어는 사람뿐만 아니라 소프트웨어, 운영자, 그리고 관리 의사 결정에도 잘못 적용된다.

소프트웨어는 "실패"하지 않는다; 단순히 작성된 로직을 실행할 뿐이다. 안전하지 않은 소프트웨어가 만들어진 이유와 – 일반적으로 요구사항 결함으로 추적될 수 있는 이유 – 안전하지 않은 소프트웨어를 만든 프로세스의 개선에 대한 권고사항 검토가 필요하다. "소프트웨어가 실패함"이라는 결론은 기술적 의미가 없으며 유용한 정보를 제공하지도 않는다.

사람도 (심장이 멈추지 않는 한) "실패"하지 않는다. 그들은 그저 자신이 처한 상황에 대응할 뿐이다. 그들이 한 일을 사후에 생각해보면 잘못 행동한 것으로 판명될 수도 있다. 그러나 유용한 권고사항을 도출하기 위해서는. 그들이 한 행동이 당시에 왜 옳은 행동으로 생각되었는지를 검토해야 한다. 다시 말해, 단순히 사람들이 잘못한 것에 대해 이야기하는 것은 사고에 대한 손쉬운 비난대상을 만드는 것 외에는 유용한 정보를 제공하지 않는다. 그들이 왜 그렇게 행동했는지를 이해하면 사고 분석에 유용한 방향으로 초점을 맞출 수 있을 것이다.

마지막으로 회사들은 사업을 중단하지 않는 한 실패하지 않는다. 사고 보고서에서 볼 수 있는 전형적인 예시는 "X 회사는 이전 사건을 통해 배우는 데 실패했다"는 문장이다. 회사는 법적실체를 설명하는 문서들의 모음에 불과하다. 문서들은 배우지 않으며, 실패하지도 않는다. 회사는 수백, 수천 또는 심지어 수만 명의 직원으로 구성될 수 있다. 왜 학습이 이루어지지 않았는지 파악하고 다음과 같은 질문을 하는 것이 더 유용할 것이다. 학습이 이루어질 수 있도록 사전에 부정적 사건을 포착하는 안전 정보 시스템(Safety Information System)이 있는가? 만약 있다면 안전 정보 시스템에 이전 사건들이 기록되어 있었는가? 그렇지 않다면, 왜 기록되지 않았는가? 그 사건들은 실수로(우연히) 누락된 것인가, 아니면 그것들을 포함시킬 프로세스가 없었던 것인가, 그것도 아니면 그 프로세스가 수행되지 않은 것인가? 만약 후자의 경우라면, 왜 그 프로세스는 수행되지 않았는가? 이전 이벤트들이 기록되었다면 왜 그 기록들은 사용되지 않았는가? 그 이벤트들은 찾기 어려웠거나 또는 반복 발생을 막기에 정보가 충분하지 않았는가? 기록된 정보를 사용하는 데 필요한 절차가 마련되어 있는가? 등등. 이러한 질문에 대한 답은 향후 이벤트에서의 학습을 향상시키고 손실의 반복을 방지하기 위한 권고사항을 만드는 데 유용한 정보를 제공할 것이다. "회사가 이벤트로부터 배우는 데 실패했다"고 단순히 결론내리는 것은 향후의 상황 개선에 필요한 정보를 제공하지 않고 책임만을 부여할 뿐이다.

"실패"의 사용을 없애면 사고로부터의 학습을 크게 향상시킬 수 있다. 우리는 "실패"가 있었다고 결론 내리지 않고 이해를 위한 탐구를 계속함으로써 사고 조사, 학습 ,그리고 바라건대 안전까지도 상당히 개선할 수 있었다.

---

[9] 시드니 데커(Sidney Dekker), A Field Guide to Understanding Human Error, London: Ashgate, 2006.

blame to the legal system. And companies and others should not be allowed to use the official accident investigations to shift liability away from themselves and onto someone else. A report that simply describes what happened, including all the contributions to the events and why, in a blame-free manner will shift the effort to assign or avoid liability to the legal process where it belongs.

## Use of Inappropriate Accident Causality Models

One other factor has a major impact on what and how much we learn from accident investigations. Many of the problems described in the previous sections stem from the definition of "cause" used in the accident analysis. It is therefore worth considering this definition a bit more. The definition of "cause" depends on the accident causality model being used in the investigation. This section answers the questions:

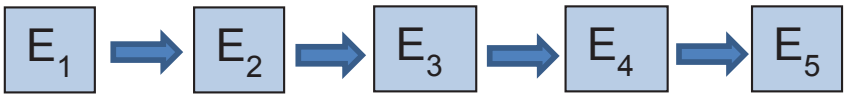
- *What is an accident causality model?*
- *What causality model is almost always used today?*
- *What are the limitations of the traditional causality model?*
- *Is there an alternative?*

*What is an accident causality model?*

A causality model simply explains why something happened. For accidents, the model is used to explain why the accident occurred. We all have a model in our heads of how and why we think accidents occur. We may not consciously think about it, but it influences our thinking. When we try to learn from and prevent accidents, we use that model in the process. If the model limits the causal mechanisms considered, then it will reduce learning.

*What causality model is almost always used today?*

The most common model of causality assumes that accidents are the result of a chain of events, where the events usually involve failures of system components and each failure or event is the direct cause of the one preceding it.




This model has been given various names and analogies used for depictions of the events (Figure 6 and Figure 7), but the underlying model is the same, that is, a chain of failure events.

더 일반적으로는, 손실로부터의 더 많이 배우기 위해 사고 보고서에서 책임을 부여하는 데 초점을 두지 않아야 하며, 이것이 어려울 수도 있다. 사고에 책임 있는 자를 찾으려는 인간의 본성이 있는 것 같다. 그러나 문제의 장본인을 식별하는 개인적 만족과 향후 더 많은 사고를 예방할 수 있는 기회를 잡는 것 사이에서 선택해야 한다. 엔지니어들은 법적인 책임 문제는 법률 시스템에 맡겨야 한다. 그리고 회사와 다른 사람들은 공식적인 사고 조사를 이용하여 법적 책임을 피하고 다른 누군가에게 법적 책임을 전가해서는 안 된다. 이벤트와 그 이유에 기여한 모든 것을 포함하여, 무엇이 일어났는지를 비난 없이 단순하게 기술하는 보고서는, 책임 할당이나 회피에 관한 일을 법적인 절차로 넘길 것이다.

## 부적절한 사고 인과관계 모델의 사용

또 다른 요소도 우리가 사고 조사를 통해 무엇을 얼마나 배우는지에 큰 영향을 미친다. 이전 섹션에서 설명한 많은 문제들은 사고 분석에서 사용된 "원인"의 정의로부터 비롯된다. 따라서 이 정의를 조금 더 살펴 볼 필요가 있다. "원인"의 정의는 조사에 사용된 사고 인과관계 모델에 따라 달라진다. 이번 섹션은 다음 질문에 대해 답한다:

- *사고 인과관계 모델이란 무엇인가?*
- *오늘날 거의 항상 사용되는 인과관계 모델은 무엇인가?*
- *전통적인 인과관계 모델의 한계는 무엇인가?*
- *다른 대안이 있는가?*

### *사고 인과관계 모델이란 무엇인가?*

인과관계 모델(causality model)은 어떤 일이 왜 일어났는지를 단순하게 설명한다. 사고에 있어, 모델은 사고가 발생한 이유를 설명하기 위해 사용된다. 우리 모두는 머릿속에 사고가 어떻게, 왜 발생했는지에 대한 모델을 가지고 있다. 우리는 그것을 의식적으로 생각하지는 않지만 이것은 우리의 사고(thinking)에 영향을 미친다. 사고(accident)로부터 배우고 그 사고를 예방하려고 할 때, 우리는 그 과정에서 인과관계 모델을 사용한다. 만약 그 모델이 고려되어야 할 인과 메커니즘(causal mechanism)을 제한한다면 그 모델은 학습을 감소시킬 것이다.

### *오늘날 거의 항상 사용되는 인과관계 모델은 무엇인가?*

가장 널리 사용되는 인과관계 모델에서는 사고가 이벤트 체인(chain of events)의 결과라고 가정하는데, 여기서 이벤트는 대개 시스템 컴포넌트의 실패를 포함하며 각 실패나 이벤트는 그 이후 이벤트의 직접적인 원인이 된다.




이 모델에서 이벤트를 기술하기 위해 사용되는 다양한 이름과 비유가 있지만(그림 6과 그림 7) 기본 모델은 동일하다. 즉, 실패 이벤트 체인(chain of failure events)이다.



**Figure 6**: Heinrich's Domino Model, 1932.

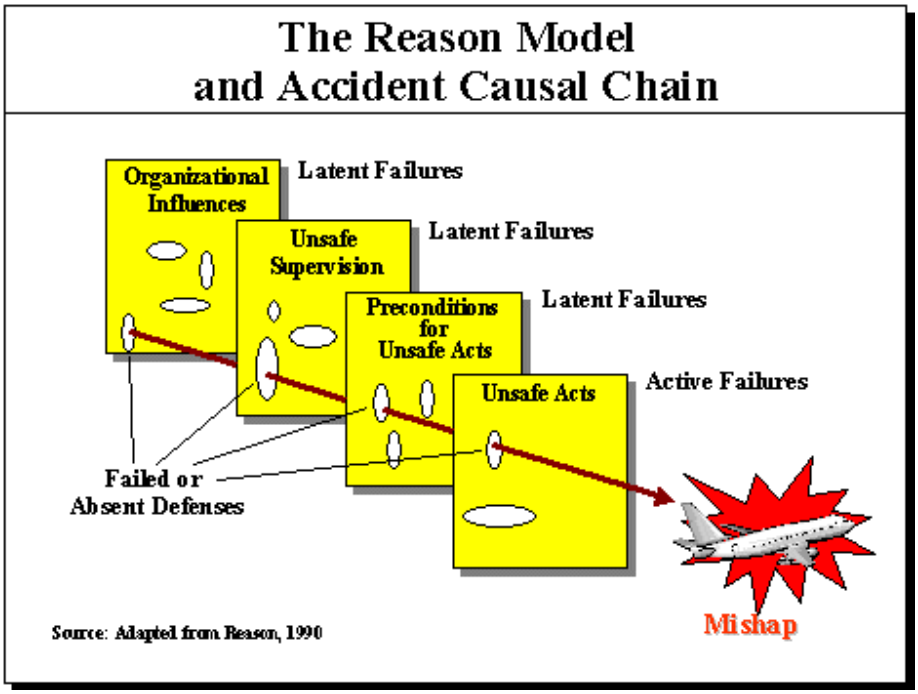



**Figure 7**: Reason's Swiss Cheese Model

As an example, consider the Bhopal (India) chemical plant release of methyl isocyanate (MIC), which killed and seriously injured tens of thousands of people. The chain of events might be stated as the following:

E1: A worker washes out pipes without inserting a slip blind to keep water isolated from MIC.

E2: Water from the pipe washing leaks into the MIC tank (MIC is explosive in the presence of water.) and pressure rises in the tank.

E3: The control room operator does not open the valve to a secondary relief tank to relieve pressure because the gauges are out of order. He thinks the relief tank is full.

E4: An explosion occurs.



그림 6: 하인리히(Heinrich)의 도미노 모델, 1932.

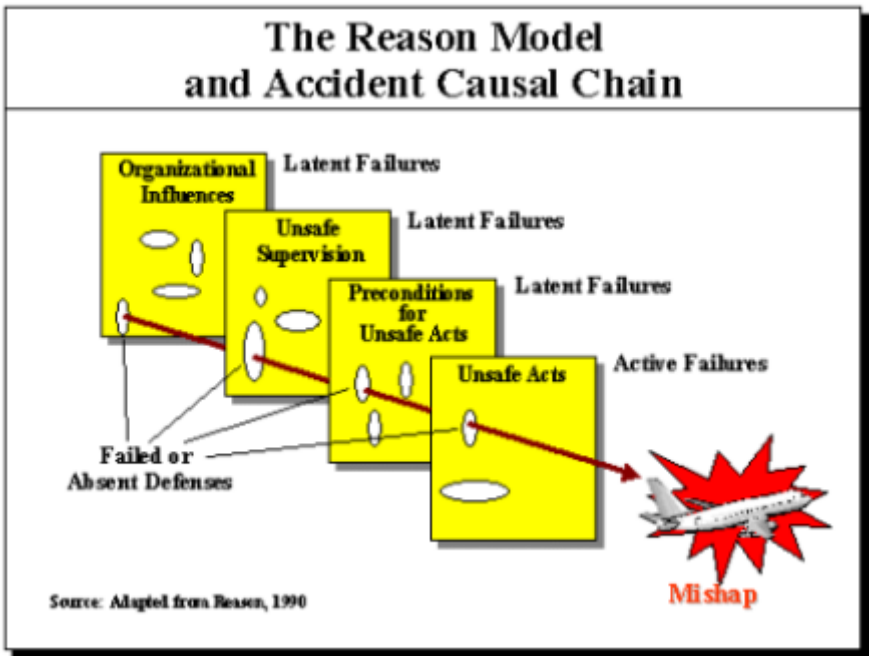



그림 7: 리즌(Reason)의 스위스 치즈 모델

예를 들어, 수만 명의 사람들을 사망하게 하고 중상을 입힌 보팔(Bhopal, 인도) 화학 공장의 메틸 이소시아네이트(MIC) 유출 사고를 보자. 이벤트 체인은 다음과 같이 기술할 수 있다.

E1: 작업자가 MIC를 물에 닿지 않게 하기 위한 슬립 블라인드(slip blind)를 삽입하지 않고 파이프를 세척한다.

E2: 파이프를 세척한 물이 MIC 탱크로 누출되고(MIC는 물에서 폭발성이 있음) 탱크의 압력이 상승한다.

E3: 제어실 운영자는 게이지가 고장 났기 때문에 압력을 줄일 수 있는 2차 릴리프 탱크로의 밸브를 열지 않는다. 그는 릴리프 탱크가 가득 차 있다고 생각한다.

E4: 폭발이 일어난다.

E5: The automated relief valve opens (as designed) in the presence of high pressure.

E6: None of the protection devices (flare tower, vent scrubber, and water curtain) prevent the release of the MIC and it is vented into the air.

E7: Wind carries MIC into the highly populated area around the plant.

From this chain of events, one event is usually selected as the root cause. In this case, both Union Carbide (the owner of the plant) and the Indian subsidiary running the plant pointed at the low-level worker who washed out the pipes without inserting a slip blind, and he was actually put in jail. Note, however, that this choice is arbitrary. Any of the other events could have been selected, such as the operators not opening the valve to the relief tank or the protection devices not working.

The chain of events here could have been followed farther back, but the chaining usually stops when a convenient person or event is found upon which to place the blame, in this case the pipe washer. The selected root cause event usually involves an operator action or inaction that is close to the time of the actual loss. Putting the worker in jail may have satisfied the goals of most everyone else involved (who were quite happy to deflect the blame away from themselves) but does not help to identify and eliminate the true causes of the accident, which were much more complex. Basically, to learn from accidents and prevent future ones, we need to know not just what events occurred but why. And the assumption that the events always occur in a simple causal chain is untrue.

For example, why did the pipe washer not insert the slip blind? In fact, the worker who had been assigned the task of washing out the pipes reportedly knew that the valves leaked, but he did not check to see whether the pipe was properly isolated because, he said, it was not his job to do so. Inserting the slip blinds was the job of the maintenance department, but the maintenance sheet contained no instruction to insert this disk. The pipe-washing operation should have been supervised by the second shift operator, but that position had been eliminated in a cost-cutting effort. Using the chain of events model, we could, of course, simply insert a previous event, such as firing the second shift supervisor, as the root cause. But that doesn't solve the problem because the chain still does not explain why this accident occurred. The accident, as is the case for most accidents when they are carefully investigated, turned out to be much more complex than just a simple chain of events. A major limitation in understanding this complex set of events and avoiding future such events derives from the oversimplification implicit in using a chain of events at all. Given the design and operating conditions of the Bhopal plant, in fact, an accident was waiting to happen:

> "However [water] got in, it would not have caused the severe explosion had the refrigeration unit [required to keep the MIC at a non-explosive temperature] not been disconnected and drained of freon [to save money], or had the gauges been properly working and monitored, or had various steps been taken at the first smell of MIC instead of being put off until after the tea break, or had the scrubber been in service, or had the water sprays been designed to go high enough to douse the emissions, or had the flare tower been working and been of sufficient capacity to handle a large excursion."[10]

And this is just the beginning. Among a large number of other things, a safety audit two years before had noted many problems at the plant, including all the ones implicated in the loss, but the identified deficiencies were never fixed. The details are unimportant here. The basic problem is that causality in complex losses cannot be captured by simple chains of events.

[10] Charles Perrow, The Habit of Courting Disaster, *The Nation*, October, 1986, p. 349

E5: (설계된 대로) 고압 상태에서 자동 릴리프 밸브가 열린다.

E6: 보호 장치(플레어 타워, 벤트 스크러버 및 워터 커튼) 중 어느 것도 MIC의 유출을 막지 못하고 MIC가 공기 중으로 퍼진다.

E7: 바람이 공장 주변의 인구 밀도가 높은 지역으로 MIC를 퍼뜨린다.

이 이벤트 체인에서 일반적으로 하나의 이벤트가 근본 원인으로 선택된다. 이 경우에서는, 유니온 카바이드(Union Carbide, 공장의 소유주)와 공장을 운영하는 인도 자회사 모두 슬립 블라인드를 삽입하지 않고 파이프를 세척한 낮은 직급의 작업자를 지적했으며, 실제로 그는 감옥에 수감되었다. 그러나 이 선택은 독단적이라는 점에 주목해야 한다. 작업자가 릴리프 탱크로의 밸브를 열지 않은 것 또는 보호 장치가 작동하지 않은 것 등 다른 이벤트를 선택할 수도 있었다.

여기서의 이벤트 체인은 좀 더 뒤까지 진행될 수 있었지만 책임을 넘기기 쉬운 사람이나 사건이 발견되면 체인이 멈추게 되는데, 이 경우 파이프 세척자가 이에 해당된다. 선택된 근본 원인 이벤트는 일반적으로 실제 손실이 발생하는 시점에서의 작업자의 행동 또는 나태함과 관련된다. 작업자를 감옥에 수감시키는 것은 관련된 대부분의 사람들(스스로 책임을 회피하는 것을 매우 기뻐했던 사람들)의 목표를 만족시켰을지 모르지만 훨씬 복잡한 사고의 진정한 원인을 식별하고 제거하는 데에는 도움이 되지 않는다. 기본적으로 사고로부터 배우고 미래의 사고를 예방하기 위해서는 어떤 이벤트가 발생했는지 뿐만 아니라 그것이 왜 발생했는지를 알아야 한다. 그리고 이벤트가 항상 단순한 원인 체인(causal chain)에서 발생한다는 가정은 맞지 않는다.

예시로, 파이프 세척자가 슬립 블라인드를 왜 삽입하지 않았을까? 실제로 파이프 세척 업무를 맡은 작업자는 밸브가 누출된 것을 알고는 있었지만, 파이프가 제대로 차단되었는지 확인하는 것은 그의 업무가 아니기 때문에 확인하지 않았다고 말했다. 슬립 블라인드를 삽입하는 것은 유지보수 부서의 일이었지만 유지보수 업무 시트에는 그 디스크(슬립 블라인드)를 삽입하라는 지시가 포함되어 있지 않았다. 파이프 세척 작업은 두 번째 교대 근무자가 감독해야 했지만 그 직위는 비용 절감을 이유로 없어졌다. 이벤트 체인 모델을 사용한다면, 우리는, 물론, 단순하게 두 번째 교대 근무자를 근본 원인(root cause)으로 보고 두 번째 교대 근무자 해고와 같은 것을 이전 단계의 이벤트로 삽입할 수도 있다. 하지만 그것은 이 사고가 왜 일어났는지 설명할 수 없기 때문에 문제는 여전히 해결되지 않는다. 대부분의 사고는 그 사고가 보다 면밀하게 조사되었을 때 단순한 이벤트 체인보다 훨씬 더 복잡한 것으로 밝혀진다. 이 복잡한 이벤트 집합을 이해하고 향후 그러한 이벤트를 피함에 있어 주요한 한계는, 이벤트 체인의 사용에 내포된 지나친 단순화로부터 비롯된다. 보팔(Bhopal) 플랜트의 설계 및 운영 조건을 고려해보면 사실 사고가 언제든 발생할 수 있었다고 할 수 있다.

> "그러나 [물]이 들어 왔더라도 냉각 장치[MIC가 폭발되지 않는 온도로 유지하기 위한]의 연결이 끊어지지 않았고 프레온이 배출되지 않았다면[비용을 절약하기 위해], 게이지가 제대로 작동 및 모니터링 되었다면, 처음 MIC의 냄새를 맡았을 때 휴식시간 이후까지 미루지 않고 여러 조치를 수행했다면, 스크러버가 작동 중이었다면, 물 분무설비(water spray)가 배기가스를 충분히 가라앉힐 수 있을 만큼 높은 곳에 있도록 설계되었다면, 플레어 타워가 작동하고 대규모 폭발을 처리할 수 있는 충분한 용량을 가지고 있었다면 심각한 폭발을 일으키지 않았을 것이다."[10]

그리고 이것은 시작에 불과하다. 다른 많은 것들이 있지만, 2년 전의 안전 감사에서는 발전소의 손실과 연관된 많은 문제를 지적했고 식별된 결함들은 고쳐지지 않았다. 여기서 자세한 내용은 중요하지 않다. 근본적인 문제는 손실에서의 복잡한 인과관계가 단순한 이벤트 체인에 의해 파악될 수 없다는 것이다.

---

[10] Charles Perrow, The Habit of Courting Disaster, The Nation, October, 1986, p.349

*What are the limitations of this traditional causality model?*

One of the most important limitations is an assumption about the linearity of accident causes. Note also that aside from the influence of one event on the next event in the chain, there is an assumption that the events are independent. In fact, there are almost always systemic causes that impact all the events in the chain.

Consider again the Bhopal accident, whose cause was identified as the worker who washed out the pipes without inserting protection against a leaky valve. Many of the poor conditions at the plant were allowed to persist because of financial pressures: Demand for MIC had dropped sharply, leading to reductions in production and pressure on the company to cut costs. In response, the maintenance and operating personnel were cut in half. Maintenance procedures were severely cut back and the shift relieving system was suspended—if no replacement showed up at the end of the shift, the following shift went unmanned. The person responsible for inserting the slip blind in the pipe had not showed up for his shift and thus he was not replaced, and nobody inserted the protection device.

As the Bhopal plant lost money, many of the skilled workers left for more secure jobs. They either were not replaced or were replaced by unskilled workers (like the pipe washer who was blamed for the accident). Staff educational standards were reduced along with training. Management and labor problems followed the financial losses, leading to low morale at the plant.

These are only a few of the factors involved in this catastrophe, which also included other technical and human errors in the plant, design errors, management negligence, regulatory deficiencies on the part of the U.S. and Indian governments, and general agricultural and technology transfer policies related to the reason such a dangerous chemical was being made in India in the first place. Any one of these perspectives or causes is inadequate by itself to understand the accident and to prevent future ones. When all the factors are considered, the pipe washing operator looks less and less likely to be the "root" or "probable" cause of this accident. Do you think that putting the pipe washer in jail (as occurred after the accident) would be effective in preventing future accidents in this plant given all the problems stated so far (and there were many more)?

Implicit in the chain of events model is an assumption of direct causality between the events in the chain, that is, A→B, which states that A is a necessary and sufficient cause of B. The contrapositive of this logical statement implies that if B does not occur, then A has not occurred. While this makes for elegant formal logic, it inhibits the comprehensive identification of accident causes when applied to the messy real world in which we all live. For example, using the contrapositive and formal definitions of event chains, it is not possible to make the statement "Smoking causes lung cancer," because not everyone who smokes gets lung cancer and not everyone who gets lung cancer smokes. In fact, the Tobacco Lobby used the contrapositive argument for decades to prevent limitations being placed on smoking and cigarettes. We know that there is a connection, but it is clearly not a simple and direct one.

Many of the systemic causes described above are only indirectly related to the proximate events preceding the loss, which by using the contrapositive rule means they could not considered to be a cause. In fact, many of these factors had an impact on *all* the events in the chain, also negating the assumption that the events are unrelated except directly through a simple chain-like relationship. Identifying the chain of events provides little help in understanding why an accident occurred and how to prevent it in the future. At best, it is only a starting point for a causal analysis. Even then, it might limit the factors considered and bias the results.

Effectively preventing accidents in complex systems requires using accident models that include the social system as well as the technology and its underlying science. Without understanding the purpose, goals, and decision criteria used to construct and operate our systems, it is not possible to completely understand and most effectively prevent accidents.

*전통적인 인과관계 모델의 한계는 무엇인가?*

가장 중요한 한계 중 하나는 사고 원인의 선형성(linearity)에 대한 가정이다. 또한 체인 내에서 다음 이벤트에 대한 한 개 이벤트의 영향 외에도 이벤트는 서로 독립적이라는 가정이 있다. 실제로 체인의 모든 이벤트에 거의 항상 영향을 미치는 시스템적 원인이 있다.

보팔 사고에서 누출된 밸브에 대해 보호 장치를 삽입하지 않고 파이프를 세척한 작업자를 원인으로 식별한 경우를 다시 생각해보자. 재정적인 압박 때문에, 플랜트의 열악한 조건 중 많은 부분이 지속되었다: MIC에 대한 급격한 수요 감소가 회사의 생산 감소 및 비용 절감 압박으로 이어졌다. 이에 따라 유지보수 및 운영 인력이 절반으로 줄었다. 유지보수 절차가 매우 축소되었고 교대 완화 시스템(shift relieving system)이 중단되었다 – 만약 교대 시점에 교대자가 나타나지 않으면 다음 교대 근무는 무인으로 진행된다. 파이프에 슬립 블라인드를 삽입하는 담당자가 교대 근무에 나오지 않았기 때문에 근무자는 교체되지 않았고 결국 아무도 보호 장치를 삽입하지 않았다.

보팔 플랜트의 재정 악화에 따라 숙련된 많은 작업자들이 보다 안정적인 일자리를 찾아 떠났다. 떠난 작업자들의 자리는 채워지지 않거나 숙련되지 않은 작업자(사고로 비난받은 파이프 세척자처럼)로 대체되었다. 직원들의 교육 수준과 훈련 수준은 낮아졌다. 재정 악화에 따라 관리 및 근로 문제가 발생했고 이는 공장의 사기 저하로 이어졌다.

이 요인들은 이번 참사와 관련된 요인 중 일부일 뿐이다. 그 외 요인에는 공장의 기술적, 인적 오류를 포함하는 설계 오류, 관리 부주의, 미국과 인도 정부의 규제 결함, 위험한 화학물질이 애초에 인도에서 만들어지던 이유와 관련된 일반적인 농업 및 기술 이전 정책도 포함된다. 이런 관점이나 원인 중 어느 하나로는 사고를 이해하고 미래의 사고를 예방하기에 충분치 않다. 모든 요인을 고려했을 때 파이프 세척자는 이 사고의 "근본(root)" 또는 "가능한(probable)" 원인이 될 가능성이 낮아 보인다. 지금까지 언급된 모든 문제(이외에도 추가적인 문제요소가 더 있을 수 있음)를 고려할 때 파이프 세척자를 감옥에 수감시키는 것이(사고 후 발생한 것) 이 공장의 향후 사고 예방에 효과적일 것이라고 생각하는가?

이벤트 체인 모델에 내포된 것은 체인의 이벤트 간, 즉, A→B 사이의 직접적인 인과관계에 대한 가정, 즉, A는 B의 필요 충분(necessary and sufficient) 원인이라는 것이다. 이 논리적 진술의 반대는 B가 발생하지 않으면 A가 발생하지 않는다는 것이다. 이것은 훌륭한 정형적 논리를 만들지만 우리 모두가 살고 있는 복잡한 현실 세계에 적용될 때에는 사고 원인의 포괄적인 식별을 방해한다. 예를 들어 이벤트 체인의 대립적, 형식적인 정의를 사용하면 "흡연이 폐암을 유발한다"는 것은 가능하지 않다. 흡연을 하는 모든 사람이 폐암에 걸리는 것은 아니며 폐암을 앓는 모든 사람이 흡연을 하는 것은 아니기 때문이다. 실제로 담배 로비 업계는 흡연과 담배에 규제를 두는 것을 막기 위해 수십 년 동안 반대 주장을 펼쳐왔다. 우리는 연관성이 있다는 것을 알고 있지만 그것은 단순하지 않으며 직접적인 연관성도 분명하지 않다.

위에서 설명한 많은 시스템적 원인은 손실 이전의 이벤트와 간접적으로만 관련이 있으며 대립 규칙(contrapositive rule)을 사용하면 원인으로 간주할 수 없다. 실제로 이러한 요인 중 다수가 체인의 *모든* 이벤트에 영향을 미쳤고, 단순한 체인과 같이 직접 연결된 이벤트를 제외하고는 다른 이벤트와 관련이 없다는 가정을 부정하였다. 이벤트 체인을 식별하는 것은 사고가 왜 발생했는지, 앞으로 어떻게 예방할 수 있는지를 이해하는 데 거의 도움이 되지 않는다. 기껏해야 원인 분석의 출발점일 뿐이다. 오히려 고려된 요인을 제한하고 결과를 편향시킬 수 있다.

복잡한 시스템에서 사고를 효과적으로 예방하려면 기술과 그것의 기초가 되는 과학뿐만 아니라 사회 시스템을 포함하는 사고(accident) 모델을 활용해야 한다. 시스템을 구축하고 운영하는 데 사용되는 목적, 목표, 결정 기준을 이해하지 못하면 사고를 완전히 이해하지 못하며 가장 효과적으로 예방할 수 없다.

*Is there an alternative?*

For a few simple accidents, the chain-of-events model may be adequate. To maximize learning from and preventing accidents in today's complex socio-technical systems, however, we need something more that will help us to more fully understand why the events occurred.

A new model of causality, which underlies CAST, provides that opportunity. STAMP (System-Theoretic Accident Model and Processes) is based on systems theory rather than traditional decomposition and reliability theory. In the latter, safety is essentially equated with the reliability of the system components.[11] Going into the technical details of STAMP is not necessary to use CAST. But it is useful to understand some important features of this new causality model.

CAST is rooted in systems thinking and systems theory. System theory, as used in engineering, was created after World War II to deal with the increased complexity of the systems starting to be built at that time. It was also independently created for biology in order to successfully understand the complexity of biological systems. In these systems, separation and independent analysis of interacting components (subsystems) distort the results for the system as a whole because the individual component behaviors are coupled in non-obvious ways. The first engineering uses of these new ideas were in the missile and early warning systems of the 1950s and 1960s. C.O. Miller introduced system theory concepts to safety starting in the 1950s. He also claimed to have been the first to use the name System Safety.

Sometimes "systems thinking" is used as an informal synonym for mathematically formal systems theory. Systems thinking is a holistic approach to analysis that focuses on how system components (physical devices, automation, humans, management, regulatory oversight, etc.) interrelate and behave over time. By using a systems approach to accident analysis, we get away from focusing on a few causal factors and instead provide a larger view of causality that can be used to identify powerful prevention measures.

Traditionally, complex systems have been decomposed into subcomponents with these subcomponents evaluated for some property of interest. The system may be separated into physical or functional properties or into chains of events over time. Then the results for each component are combined to get a result for the system as a whole. There are some assumptions upon which the utility of this process is based: the system components are assumed to operate independently and that separation into pieces (decomposition) does not distort the phenomenon being considered. This implies that the interactions among components can be examined pairwise, thus allowing them to be individually measured and combined to create a system value for the phenomenon. All of this also implies that the components (or events in a chain) are not subject to feedback loops and non-linear interactions.

System Theory was created in response to the fact that after WW II, our systems were becoming so complex that decomposition no longer worked (although that has not stopped people from using it). The assumptions underlying the decomposition approach just do not hold in today's software-intensive and complex systems. Instead, using System Theory:

- The system is treated as a whole, not as the sum of its parts. You have probably heard the common statement: "the whole is more than the sum of its parts."
- A primary concern is *emergent properties* (see Figure 8), which are properties that are not in the summation of the individual components but "emerge" when the components interact. Emergent properties can only be treated adequately by taking into account all their technical and social aspects. Safety is an emergent property as is security and other important engineered system properties.

[11] Nancy Leveson, *Engineering a Safer World*, MIT Press, 2012.

*다른 대안이 있는가?*

일부 단순 사고의 경우 이벤트 체인 모델이 적합할 수 있다. 그러나 오늘날 복잡한 사회-기술적 시스템에서 사고로부터 배우고 예방하는 것을 극대화하기 위해서는 그 이벤트가 왜 발생했는지를 완전히 이해하기 위한, 도움이 될 무언가가 더 필요하다.

CAST의 기초가 되는 새로운 인과관계 모델은 그러한 기회를 제공한다. STAMP(System- Theoretic Accident Model and Processes)는 전통적인 분해 및 신뢰성 이론이 아닌 시스템 이론에 기초한다. 전자의 경우, 안전은 본질적으로 시스템 컴포넌트의 신뢰성과 동일시된다.[11] CAST를 사용하기 위해 STAMP의 기술적 세부사항을 살펴볼 필요는 없지만, STAMP에 대한 기술적 이해는 이 새로운 인과관계 모델의 몇 가지 중요한 특징을 이해하는 데에는 유용할 것이다.

CAST는 시스템적 사고(systems thinking)와 시스템 이론에 뿌리를 두고 있다. 엔지니어링에 사용된 시스템 이론은 제2차 세계 대전 이후, 그 당시 구축되기 시작한 시스템의 복잡성을 다루기 위해 만들어졌으며, 이와는 독립적으로 생물학적 시스템의 복잡성을 제대로 이해하기 위해서도 만들어졌다. 상호작용하는 컴포넌트(하위 시스템)를 분리하여 독립적으로 분석하게 되면, 시스템 전체의 결과를 왜곡하게 된다. 개별 컴포넌트의 동작이 불명확한 방식으로 결합되기 때문이다. 이러한 새로운 아이디어를 처음으로 엔지니어링에 사용한 것은 1950년대와 1960년대의 미사일 및 조기 경고 시스템이었다. 밀러(Miller C.O.)는 1950년대부터 안전에 대해 시스템 이론 개념을 도입했으며 시스템 안전(system safety)이라는 단어를 처음으로 사용했다고 주장했다.

때때로 "시스템적 사고"는 수학적으로 정형적 시스템 이론의 비공식적인 동의어로 사용된다. 시스템적 사고는 시스템 구성요소(물리적 장치, 자동화, 사람, 관리, 규제 감독 등)가 시간의 흐름에 따라 상호작용하고 동작하는 방법에 초점을 맞춘 포괄적 접근법이다. 사건 분석에 시스템 접근법을 사용함으로써, 우리는 몇 가지 원인 요소에만 초점을 맞추지 않고, 강력한 예방 조치를 식별할 수 있는 인과관계에 대한 더 큰 시각을 가질 수 있다.

전통적인 분석 방법에서 복잡한 시스템은 관심 있는 속성 몇 개에 따라 평가된 서브 컴포넌트로 분해되었다. 여기서 시스템은 물리적 또는 기능적 특성에 따라 분리되거나 시간의 흐름에 따른 이벤트 체인으로 분리될 수 있다. 그런 다음 각 컴포넌트의 결과를 조합하여 시스템 전체에 대한 결과를 얻는다. 이러한 프로세스를 사용하는 데에는 다음의 몇 가지 가정이 있다: 시스템 컴포넌트는 독립적으로 동작한다고 가정하므로 낱개로 분리하는 것(분해)은 고려중인 현상을 왜곡시키지 않는다. 이는 컴포넌트 간의 상호작용을 쌍(pairwise)으로 확인할 수 있으므로 개별적으로 측정하고 결합하여 현상에 대한 시스템 값을 생성할 수 있음을 의미한다. 이 모든 것은 또한 컴포넌트(또는 체인에서의 이벤트)가 피드백 루프 및 비선형적 상호작용과 관련이 없음을 의미한다.

시스템 이론은 2차 세계대전 이후 시스템이 너무 복잡해져서 (비록 사람들은 분해 방식을 계속 사용하였지만) 분해가 더 이상 의미 없다는 사실에 대응하여 만들어졌다. 분해 접근법의 기본 가정은 오늘날의 소프트웨어 집약적이고 복잡한 시스템에는 적용되지 않으므로, 대신, 시스템 이론을 적용한다.

- 시스템을 부분들의 합으로서가 아닌 전체로서 취급한다. 당신은 아마 "전체가 그 부분의 합보다 더 크다"라는 통설을 알 것이다.
- 주요 관심사는 개별 컴포넌트의 합이 아니고 컴포넌트가 상호작용할 때 "발현(emerge)"하는 특성인 *발현 속성*(그림 8 참조)이다. 발현 속성은 모든 기술적, 사회적 측면을 고려할 때 비로소 적절하게 취급될 수 있다. 안전은 보안 및 기타 중요한 엔지니어링 시스템 속성과 마찬가지로 발현 속성을 가진다.

[11] Nancy Leveson, Engineering a Safer World, MIT Press, 2012

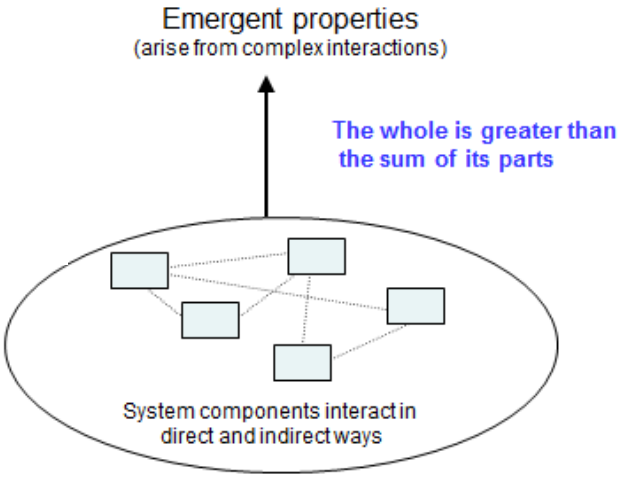



**Figure 8:** Emergent properties in system theory

- Emergent properties arise from the relationships among the parts of the system, that is, by how they interact and fit together.

If emergent properties arise from individual component behavior and complex interactions among components, then it makes sense that controlling emergent properties, such as safety, requires controlling both the behavior of the individual components and the interactions among the components. We can add a controller to the system to accomplish this goal. The controller provides control actions on the system and gets feedback to determine the impact of the control actions. In engineering, this is a standard feedback control loop (see Appendix E).

The controller *enforces constraints on the behavior of the system*. Example safety constraints might be that aircraft or automobiles must remain a minimum distance apart, pressure in deep water wells must be kept below a safe level, aircraft must maintain sufficient lift to remain airborne unless landing, toxic substances must never be released from a plant, and accidental detonation or launch of weapons must never occur.

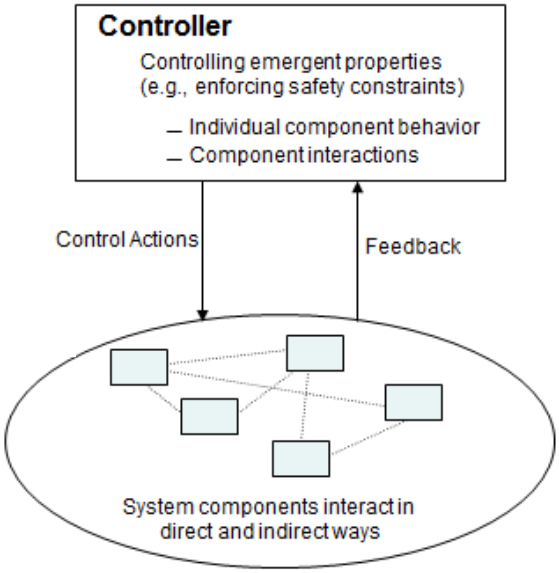



**Figure 9:** Controllers enforce constraints on behavior

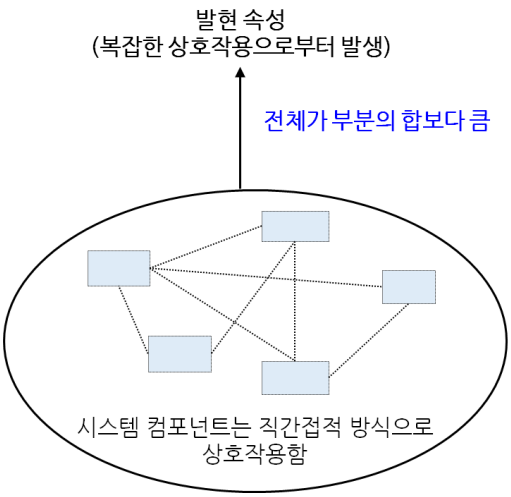



그림 8: 시스템 이론에서의 발현 속성

- 발현 속성은 시스템의 각 부분들 간의 관계, 즉, 어떻게 상호작용하고 조화하는지에 따라 발생한다.

발현 속성이 개별 컴포넌트 동작과 컴포넌트 간의 상호작용에 의해 발생한다면 안전과 같은 발현 속성을 제어하기 위해서는 개별 컴포넌트의 동작과 컴포넌트 간의 상호작용을 모두 제어해야 한다. 이러한 목적을 달성하기 위해 시스템에 컨트롤러를 추가할 수 있다. 컨트롤러는 시스템에 컨트롤 액션을 제공하고 피드백을 받아 컨트롤 액션에 따른 영향을 파악한다. 엔지니어링에서 이것이 표준 피드백 컨트롤 루프이다(부록 E 참조).

컨트롤러는 *시스템의 동작에 안전 제약사항(safety constraints)을 강제한다*. 안전 제약사항의 예로는 '항공기 또는 자동차는 최소한의 거리를 유지해야 한다', '깊은 우물의 압력은 안전한 수준 이하로 유지되어야 한다', '항공기는 착륙하지 않는 한 충분한 양력을 유지해야 한다', '플랜트에서 독성 물질이 절대로 유출되면 안 된다', '무기는 결코 우연히 폭발하거나 발사되면 안 된다' 등이 있다.

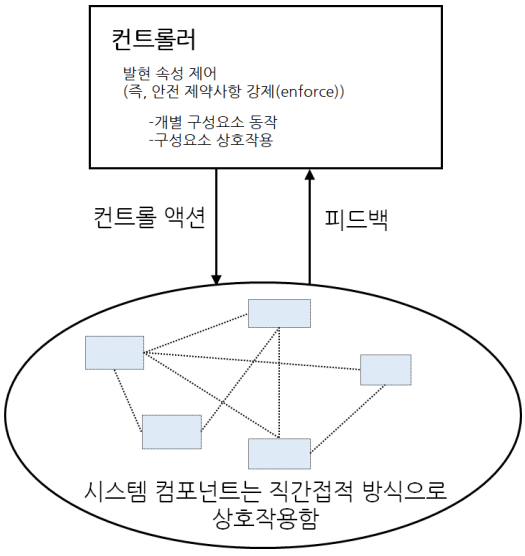



그림 9: 컨트롤러가 동작에 제약사항 강제

Control is interpreted broadly and, therefore, includes everything that is currently done in safety engineering, plus more. For example, component failures and unsafe interactions may be controlled through design, such as using redundancy, interlocks, barriers, or fail-safe design. Safety may also be controlled through processes, such as development and training processes, manufacturing processes and procedures, maintenance processes, and general system operating processes. Finally, safety may be controlled using social controls including government regulation, culture, insurance, law and the courts, or individual self-interest. Human behavior can be partially controlled through the design of a societal or organizational incentive structure or other management processes.

The safety control structure enforces the safety constraints. Responsibility for enforcing specific behavior on the system is distributed throughout the system's control structure. Figure 10 is a generic example. Accidents result from inadequate enforcement of the system safety constraints in the operation of the system as a whole. In other words, weaknesses in the safety control structure leads to violation of system safety constraints and thus losses.

Handling complex sociotechnical systems requires modeling and analyzing both the social and technical aspects of the problem and allows a combined analysis of both. Figure 10 shows an example of a hierarchical safety control structure for a typical regulated industry in the United States. International controllers may be included. The operating process (the focus of most accident analysis) in the lower right of the figure makes up only a small part of the safety control structure.

There are two basic hierarchical control structures shown in Figure 10—one for system development (on the left) and one for system operation (on the right)—with interactions between them. Each level of the structure contains controllers with responsibility for controlling the interactions between and the behavior of the components on the level below. Higher level controllers may provide overall safety policy, standards, and procedures (downward arrows), and get feedback (upward arrows) about their effect through various types of reports, including incident and accident reports. For example, company management provides safety policy, standards, and resources and gets feedback in the form of reports about the operation of the company. The feedback provides the ability to learn and to improve the effectiveness of the safety controls.

Manufacturers must communicate to their customers the assumptions about the operational environment in which the original safety analysis was based, e.g., maintenance quality and procedures, as well as information about safe operating procedures. The operational environment, in turn, provides feedback to the manufacturer and potentially others, such as governmental authorities, about the performance of the system during operations. Each component in the hierarchical safety control structure has responsibilities for enforcing safety constraints appropriate for that component, and together these responsibilities should result in enforcement of the overall system safety constraints.

Note that the use of the term "control" does not imply a rigid command and control structure. Behavior is controlled not only by engineered systems and direct management intervention, but also indirectly by policies, procedures, shared value systems, and other aspects of the organizational culture. All behavior is influenced and at least partially "controlled" by the social and organizational context in which the behavior occurs. "Engineering" this context can be an effective way to create and change a safety culture, i.e., the subset of organizational or social culture that reflects the general attitude about safety by the participants in the organization or society.[12] More about the practical implications is provided later in the handbook.

[12] Edgar Shein, *Organizational Culture and Leadership*, San Francisco: Jossey Bass, 2004

컨트롤은 광범위하게 해석되며, 그런 까닭에, 현재 안전 공학에서 수행되는 모든 것과 그 이상의 것을 포함한다. 예를 들어 다중화, 인터락(interlock), 배리어(barrier) 또는 페일세이프(fail-safe)와 같은 설계를 통해 컴포넌트의 실패와 안전하지 않은 상호작용을 컨트롤 할 수 있다. 또한 개발 및 훈련 프로세스, 제조 프로세스 및 절차, 유지보수 프로세스, 일반적인 시스템 운영 프로세스와 같은 프로세스를 통해 안전을 컨트롤 할 수 있다. 마지막으로 안전은 정부 규제, 문화, 보험, 법 및 법원 또는 개인의 사적 이익을 포함한 사회적 제어를 사용하여 컨트롤 될 수 있다. 사람의 행동은 사회적 또는 조직적 인센티브 구조나 다른 관리 프로세스의 설계를 통해 부분적으로 컨트롤 될 수 있다.

안전 컨트롤 스트럭처는 안전 제약사항을 강제한다. 시스템의 특정 동작을 강제하는 책임은 시스템의 컨트롤 스트럭처 전체에 흩어져있다. 그림 10은 일반적인 예시이다. 사고(accident)는 전체 시스템 운영에서 시스템 안전 제약사항을 부적절하게 강제하는 경우 발생한다. 다시 말해 안전 컨트롤 스트럭처의 취약점은 시스템 안전 제약사항의 위반과 이로 인한 손실을 야기한다.

복잡한 사회 기술적 시스템을 다루기 위해서는 문제에 대한 사회적, 기술적 측면을 함께 모델링하고 그 두 가지를 종합적으로 분석할 수 있어야 한다. 그림 10은 미국 규제 산업의 계층적 안전 컨트롤 스트럭처에 대한 전형적인 예시이다. 여기에는 국제적인 컨트롤러가 포함될 수도 있다. 그림의 우측 하단에 있는 운영 프로세스(대부분의 사고 분석 초점)는 안전 컨트롤 스트럭처의 일부분에 불과하다.

그림 10은 시스템 개발을 위한 스트럭처(왼쪽)와 시스템 운영을 위한 스트럭처(오른쪽)의 두 가지 기본 계층적 컨트롤 스트럭처 그리고 이들 간의 상호작용을 보여준다. 스트럭처의 각 레벨에는 하위 레벨 컴포넌트 간 상호작용 및 동작을 컨트롤 할 책임이 있는 컨트롤러가 포함되어 있다. 상위 레벨 컨트롤러는 전반적인 안전 정책, 표준 및 절차를 제공하고(아래 방향 화살표) 사건 및 사고 보고서 등의 다양한 유형의 보고서를 통해 그 효과를 피드백 받을 수 있다(윗 방향 화살표). 예를 들어 회사 관리자는 안전 정책, 표준 및 자원을 제공하고 회사 운영에 대해 보고서 형태로 피드백을 받는다. 이 피드백을 통해 안전 컨트롤의 효과를 배우고 개선할 수 있다.

제조업체는 고객에게 안전 운영 절차에 대한 정보뿐만 아니라 유지보수 품질 및 절차와 같은 원래의 안전 분석의 기반이 되는 운영 환경에 대한 가정도 알려주어야 한다. 그 운영 환경은 결국 제조업체나 다른 기관(정부 기관과 같은)에게 시스템 운영 성능에 대한 피드백을 제공한다. 계층적 안전 컨트롤 스트럭처의 각 컴포넌트는 해당 컴포넌트에 적합한 안전 제약사항을 시행할 책임이 있으며 이러한 책임은 전체 시스템에 대한 안전 제약사항의 시행으로 이어져야 한다.

"컨트롤"이라는 용어가 융통성 없는 명령이나 컨트롤 스트럭처를 의미하는 것은 아니라는 점에 유의해야 한다. 동작은 엔지니어링된 시스템이나 직접적인 관리 개입에 의해 컨트롤 될 뿐만 아니라 정책, 절차, 공유된 가치 체계(systems) 및 조직 문화의 다른 측면에 의해서도 간접적으로 컨트롤된다. 모든 동작은 그 동작이 일어나는 사회적, 조직적 컨텍스트에 의해 영향을 받으며 적어도 부분적으로라도 "컨트롤"된다. 이러한 컨텍스트를 "엔지니어링" 하는 것은 안전 문화를 만들고 변화시키는 데 효과적인 방법이 될 수 있다. 안전 문화는 안전에 대한 조직이나 사회 구성원들의 일반적 태도를 반영하는 조직적 또는 사회적 문화의 부분 집합이다.[12] 실질적인 영향에 대한 자세한 내용은 핸드북 뒷부분에서 제시한다.

[12] Edgar Shein, *Organizational Culture and Leadership*, San Francisco: Jossey Bass, 2004

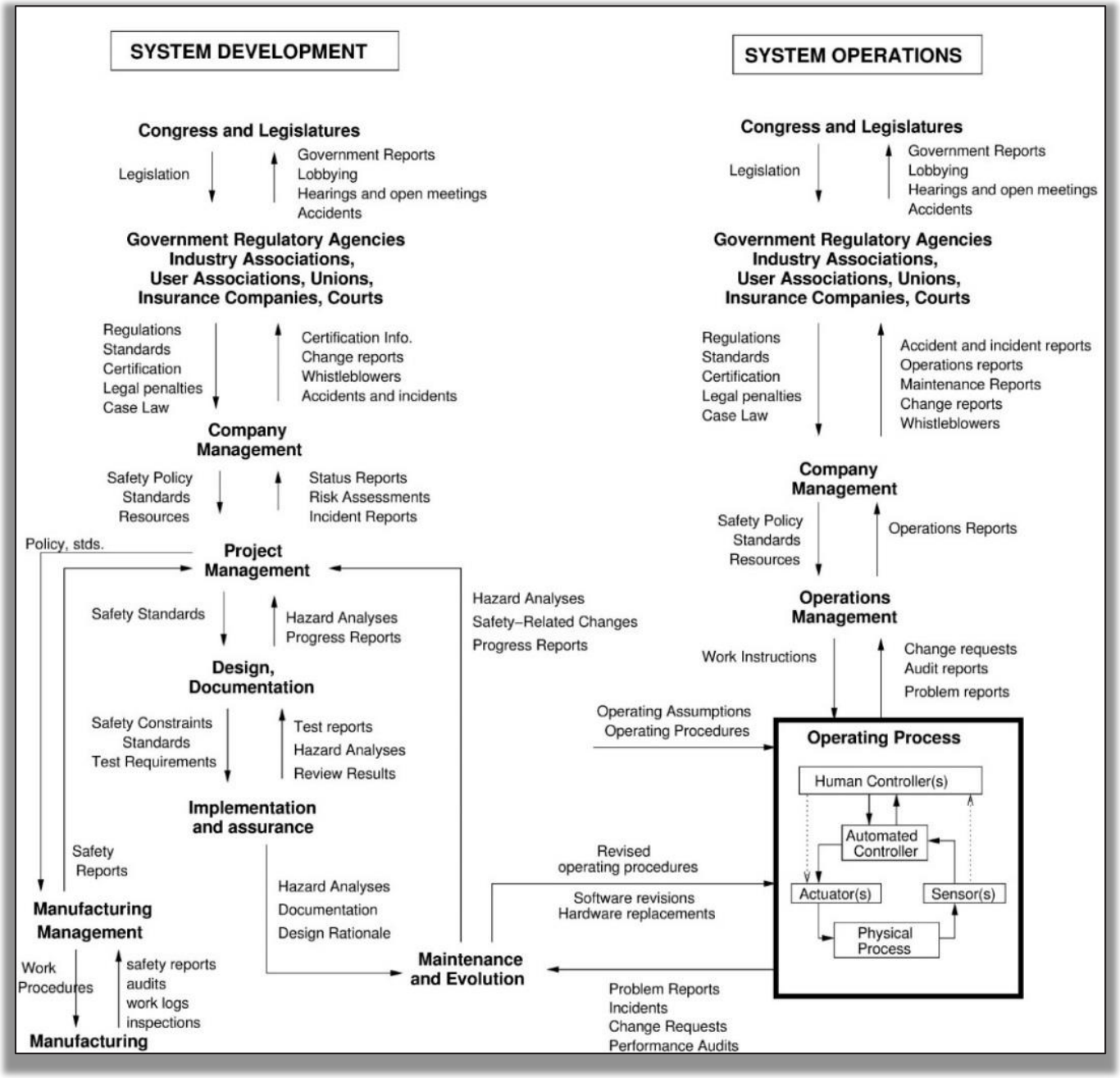



**Figure 10**: A generic safety control structure

As we have learned from major accidents, managerial and organizational factors and often governmental controls (or lack of them) are as important as technical factors in accident causation and prevention. For space reasons, Figure 10 emphasizes the high-level components of a safety control structure and not their detailed design. Each can be quite complex and needs to be examined comprehensively to understand why an accident occurred.

Figure 11 shows the basic form of the interactions between the levels of the control structure, where the controller imposes control actions on the controlled process. In engineering, this is called a feedback control loop. The standard requirements for effective management—assignment of responsibility, authority, and accountability—are part of the control structure design and specification as shown.

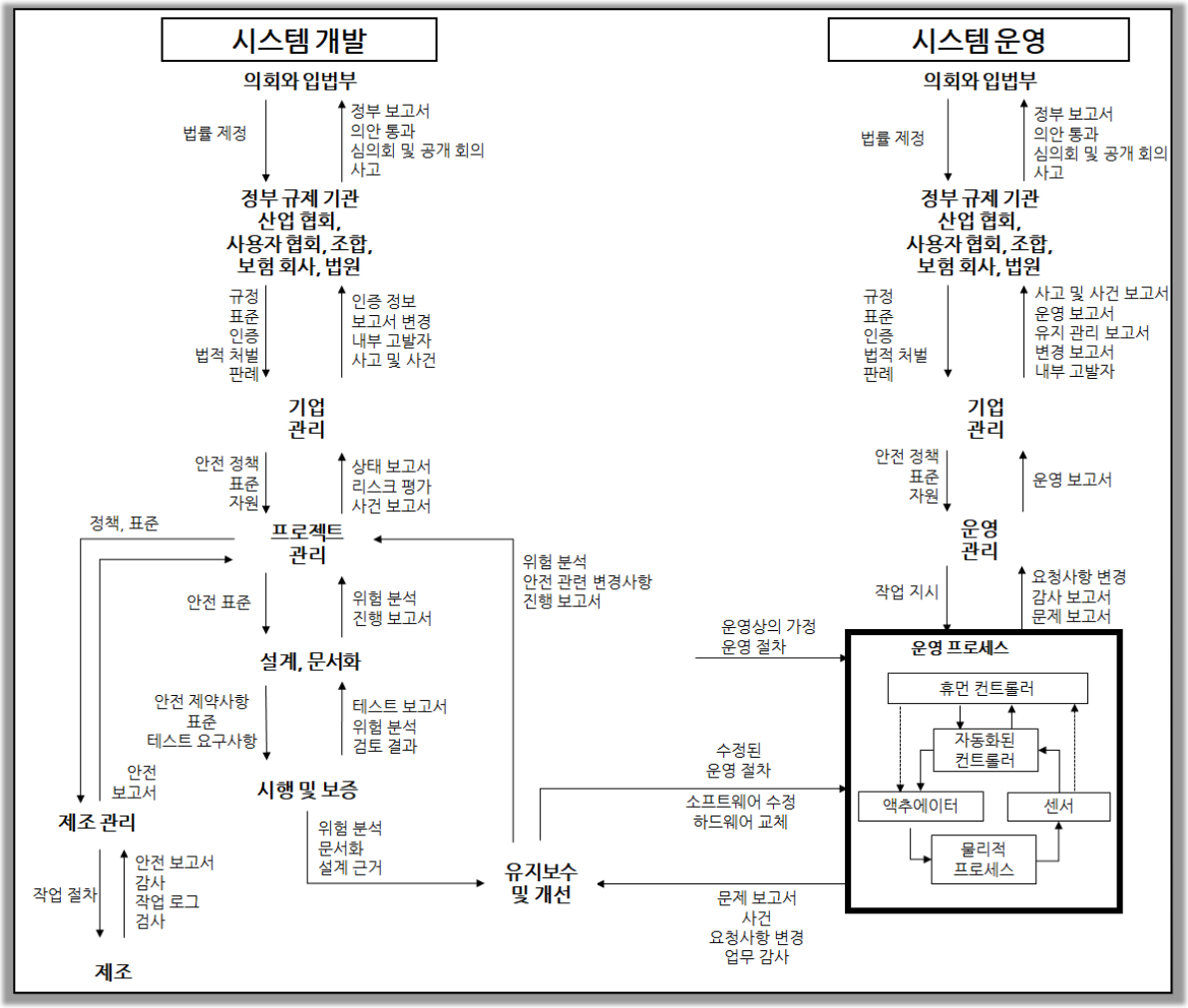



그림 10: 일반적인 안전 컨트롤 스트럭처

주요 사고에서 알게 된 바와 같이 관리적, 조직적 요인 및 정부 통제(또는 통제 부족)는 사고 원인과 예방의 기술적 요인만큼 중요하다. 지면상 제약으로 인해 그림 10에서는 안전 컨트롤 스트럭처의 상세 설계가 아닌 상위 레벨 컴포넌트를 강조하였다. 각 요소는 매우 복잡할 수 있기 때문에 사고 발생 이유를 이해하기 위해서는 종합적 검토가 필요할 것이다.

그림 11은 컨트롤 스트럭처의 각 레벨 간 상호작용에 대한 기본적인 형태를 보여주며 여기서 컨트롤러는 컨트롤드 프로세스(controlled process)에 컨트롤 액션(control action)을 제공한다. 엔지니어링에서는 이것을 피드백 컨트롤 루프(feedback control loop)라고 한다. 책임(responsibility), 권한(authority) 및 의무(accountability)의 할당과 같은 효과적인 관리를 위한 표준 요구사항은 그림과 같이 컨트롤 스트럭처 및 명세에 포함된다.

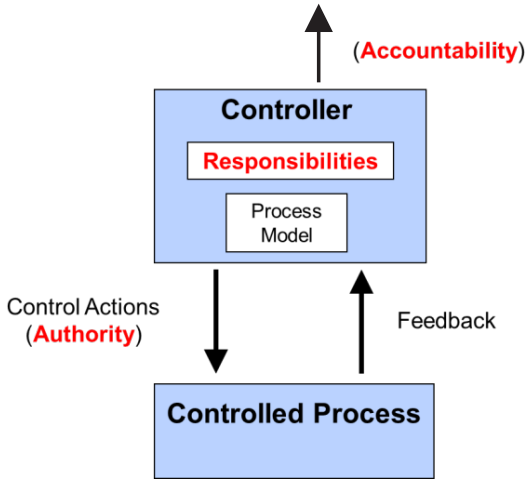



**Figure 11**: The basic building block for a safety control structure

The controller has responsibilities assigned to it with respect to enforcing the system safety constraints, for example, providing commands to an aircraft's control surfaces to control lift or, in a chemical plant, to open and close valves to maintain a safe level of pressure in a tank. The controller (which may be a human or automation) satisfies these responsibilities by issuing control actions on the process it is controlling (representing its authority). The controller determines what type of control actions are required to satisfy its responsibilities for preventing hazards given the current state of the controlled process, which is identified through feedback from the process being controlled.

As an example of a higher-level controller, the FAA has responsibilities related to overseeing the safety of flight in the U.S. The agency has various types of control actions to carry out its responsibilities, such as airworthiness advisory circulars and directives, FAA regulations, handbooks and manuals, Notices to Airmen (NOTAMs), policy and guidance, etc. Feedback comes in the form of reporting systems, accident and incident analysis, audits and inspections, etc. to determine the current state of safety of the air transportation system. Ultimately, the FAA is accountable to the Dept. of Transportation, Congress, and the public.

Feedback information is incorporated into the controller's model of the controlled process, called the *process model* or, if the controller is a human, it may be called the *mental model*. Accidents often result when the controller's process model becomes inconsistent with the actual state of the process and the controller provides unsafe control as a result. For example, the air traffic controller thinks that two aircraft are not on a collision course and does not change the course of one or both. Other examples are that the manager of an airline believing the pilots have adequate training and expertise to perform a particular maneuver safely when they do not, or a pilot thinking that de-icing has been accomplished when it has not.

In a simple feedback control loop, the controllers implement a control action, such as pulling back on the yoke in an aircraft or opening a valve in a plant. An "actuator" (not shown for simplicity) implements that control action in the controlled process. Feedback is usually designed into the system so that the controller can determine the effect of their control action and decide what to do next.

The importance of feedback becomes apparent here. Feedback informs the current process (or mental) model, which the controller uses to determine what control actions are needed. In engineering, every controller must contain a model of the controlled process in order to provide effective control. This process model or mental model includes assumptions about how the controlled process operates and the current state of the controlled process. It is used to determine what control actions are necessary to keep the system operating effectively. For example, the mental model of a pilot may

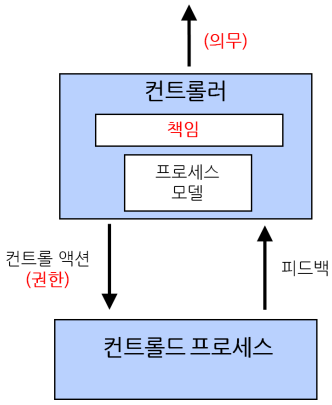



그림 11: 안전 컨트롤 스트럭처의 기본 빌딩 블록

컨트롤러는 시스템 안전 제약사항을 강제하는 책임을 갖는다. 예를 들면 항공기 조종익면(control surface)을 제어하기 위한 명령을 제공하거나 화학 공장에서 밸브를 열고 닫아서 탱크의 압력을 안전한 수준으로 유지하기 위한 명령을 제공한다. 컨트롤러(사람 또는 자동화 일 수 있음)는 그 컨트롤러를 컨트롤 중인(권한을 나타내는) 프로세스에 대해 컨트롤 액션을 제공함으로써 이러한 책임을 만족시킨다. 컨트롤러는 컨트롤되는 프로세스의 피드백을 통해 식별되는 컨트롤드 프로세스의 현재 상태를 식별하고, 현 상태에서 어떤 유형의 컨트롤 액션이 필요한지를 결정함으로써 위험을 방지하기 위한 책임을 만족시킨다.

상위 레벨 컨트롤러의 예로 FAA(Federal Aviation Administration)는 미국 내 비행 안전 감독과 관련된 책임을 가지고 있다. 이 기관은 감항(airworthness) 권고사항(AC) 및 명령, FAA 규정, 핸드북 및 매뉴얼, 항공 고시보(NOTAM), 정책 및 지침과 같은 책임을 수행하기 위한 다양한 유형의 컨트롤 액션을 가지고 있다. 피드백은 항공 운송 시스템의 현재 안전 상태를 파악하기 위한 보고시스템, 사고 및 사건 분석, 감사 및 조사 등의 형태로 제공된다. 궁극적으로 FAA는 교통부, 의회, 대중에 대한 책임이 있다.

피드백 정보는 *프로세스 모델*이라고 불리거나 컨트롤러가 사람인 경우에는 *멘탈 모델*이라고 불리며 컨트롤드 프로세스의 컨트롤러 모델에 포함되어 있다. 사고는 종종 컨트롤러의 프로세스 모델이 프로세스의 실제 상태와 일치하지 않아 결과적으로 컨트롤러는 안전하지 않은 컨트롤을 제공할 때 발생한다. 예를 들면 항공 교통 관제사가 두 항공기가 충돌 코스에 있지 않다고 생각해서 둘 중 한 항공기 또는 항공기 둘 모두의 코스를 바꾸지 않는 것이다. 다른 예로 항공사 관리자가 특정 기동(maneuver)을 안전하게 수행할 수 있는 적절한 훈련과 전문 지식을 가지고 있지 않은 조종사에 대해 그렇다고 믿는 것 또는 제빙이 되지 않았는데 조종사가 제빙이 이루어졌다고 생각하는 것 등이 있다.

간단한 피드백 컨트롤 루프에서 컨트롤러는 항공기의 요크(yoke)를 뒤로 당기거나 플랜트에서 밸브를 여는 것과 같은 컨트롤 액션을 수행한다. “액추에이터”(단순화를 위해 생략됨)는 컨트롤드 프로세스에서 컨트롤 액션을 수행한다. 피드백은 일반적으로 시스템 내에 설계되어 컨트롤러가 컨트롤 액션의 효과를 확인하고 다음에 무엇을 할지 결정할 수 있도록 한다.

여기서 피드백의 중요성이 명백해진다. 피드백은 현재의 프로세스(또는 멘탈) 모델에게 정보를 제공하며, 이 정보는 컨트롤러가 어떤 컨트롤 액션이 필요한지 결정하기 위해 사용된다. 엔지니어링에서 모든 컨트롤러는 효과적인 컨트롤을 제공하기 위해 컨트롤드 프로세스 모델을 가져야 한다. 이 프로세스 모델 또는 멘탈 모델에는 컨트롤드 프로세스가 작동하는 방법과 컨트롤드 프로세스의 현재 상태에 대한 가정이 포함된다. 그 가정은 시스템을 효과적으로 작동시키기 위해 어떤 컨트롤 액션이 필요한지를 결정하는 데 사용된다. 예를 들어 조종사의 멘탈 모델에는 자세 및 조종익면(control surface)의 상

include information about the physical aircraft, such as the attitude and the state of the control surfaces. If the aircraft has control automation (true for almost all aircraft today), the pilot has to have information about how that automation works and the current state of the automation such as the operating mode. The automation also has a model of the process state, such as the current state of the physical control structures.

Accidents in complex systems often result from inconsistencies between the model of the process used by the controller and the actual process state, which results in the controller providing unsafe control actions. For example, the autopilot software thinks the aircraft is climbing when it really is descending and applies the wrong control law; a military pilot thinks a friendly aircraft is hostile and shoots a missile at it; the software thinks the spacecraft has landed and turns off the descent engines prematurely; the early warning system thinks the country has been targeted by someone with hostile intent and launches an interceptor at a friendly target. Note that it does not matter whether the incorrect process model was a result of an unintentional or intentional cause, which means that security can be handled in the same way. The Stuxnet worm in the Iranian reactor program is an example. The worm made the controller's process model think that the centrifuges were spinning slower than they were. The controller reacted by sending "increase speed" commands to the centrifuges, wearing them out prematurely and slowing down the Iranian development of nuclear weapons.

Part of the challenge in designing an effective safety control structure is providing the feedback and inputs necessary to keep the controller's model of the controlled process consistent with the actual state of the controlled process. An important component in understanding why accidents and losses occurred involves determining how and why the controls were ineffective in enforcing the safety constraints on system behavior. Often this is because the process model used by the controller was incorrect or inadequate in some way.

To summarize: Using systems theory, an accident results not from failures of system components, but by the inability of the safety control structure to maintain constraints on the behavior of the system. For example, there is insufficient lift to keep the aircraft airborne or insufficient distance from fixed terrain is maintained to avoid a collision. Physical failures may occur and lead to inadequate control, but there are many more things to consider.

To apply system theory to safety, a new accident causality model is required that extends what is currently used. STAMP (System-Theoretic Accident Model and Processes) expands the traditional model of causality beyond a chain of directly-related failure events or component failures to include more complex processes and unsafe interactions among system components.[13] In STAMP, accidents are caused by complex interactions among physical systems, humans, and social systems. Safety is treated as a dynamic control problem rather than a failure prevention problem. No causes are omitted from the STAMP model (event-chain models are a subset), but more are included and the emphasis changes from preventing failures to enforcing constraints on system behavior.

Some advantages of using STAMP are:

- It applies to very complex systems because it works top-down from a high level of abstraction rather than bottom up.
- It includes software, humans, organizations, safety culture, etc. as causal factors in accidents and other types of losses without having to treat them differently or separately.

STAMP is the accident causality model that underlies CAST.

[13] See Nancy G. Leveson, *Engineering a Safer World*, MIT Press (2012), Cambridge MA.

태와 같은 물리적 항공기에 대한 정보가 포함될 수 있다. 만약 항공기의 컨트롤이 자동화되어 있다면 (오늘날 거의 모든 항공기가 그러함) 조종사는 그 자동화가 어떻게 작동하는지에 대한 정보, 운영 모드와 같은 자동화의 현재 상태 정보를 가지고 있어야 한다. 또한 자동화는 물리적 컨트롤 스트럭처의 현재 상태와 같은 프로세스 상태 모델을 가지고 있다.

복잡한 시스템에서의 사고는 종종 컨트롤러가 사용하는 프로세스 모델과 실제 프로세스 상태 사이의 불일치로 인해 컨트롤러가 안전하지 않은 컨트롤 액션을 제공하여 발생한다. 예를 들어 항공기가 실제로는 하강하고 있고 자동 조종 소프트웨어는 항공기가 상승하고 있다고 판단하여 잘못된 컨트롤을 적용한다; 군 조종사가 아군 항공기를 적이라고 생각하여 미사일을 발사한다; 소프트웨어가 우주선이 착륙했다고 생각하여 하강 엔진을 너무 빨리 꺼버린다; 적대적인 의도를 가진 누군가가 특정 지역을 겨냥하였다고 판단하여 조기 경고 시스템이 아군 타겟에 요격기를 발사한다. 잘못된 프로세스 모델이 의도하지 않은 원인에 대한 결과인지, 의도한 원인에 대한 결과인지 여부는 중요하지 않다. 보안도 동일한 방식으로 다루어 질 수 있다. 이란 원자로(reactor) 프로그램의 스턱스넷 웜(Stuxnet worm)이 그 예다. 이 웜은 컨트롤러의 프로세스 모델로 하여금 원심분리기가 원래보다 느리게 회전하고 있다고 생각하게 만들었다. 컨트롤러는 원심분리기에 "속도 증가" 명령을 보내어 그 원심분리기가 빨리 마모되게 하였고 결과적으로 이란의 핵무기 개발이 늦춰졌다.

효과적인 안전 컨트롤 스트럭처 설계에 있어 어려운 것 중 하나는, 컨트롤드 프로세스의 컨트롤러 모델을 컨트롤드 프로세스의 실제 상태와 일치시키는 데 필요한 피드백 및 입력을 제공하는 것이다. 사고와 손실이 발생한 이유를 이해하기 위해서는 컨트롤이 시스템 동작에 안전 제약사항을 강제하는 것이 효과적이지 않았던 이유와 방법을 파악하는 것이 중요하다. 이는 컨트롤러가 사용하는 프로세스 모델이 어떤 식으로든 잘못되었거나 부적절할 수 있기 때문이다.

요약하자면: 시스템 이론을 활용하면 사고는 시스템 컴포넌트의 실패 때문에 발생하는 것이 아니라 안전 컨트롤 스트럭처가 시스템의 동작에 대한 제약사항을 유지할 수 없기 때문에 발생한다. 예를 들면 항공기의 비행을 유지하기 위한 양력이 충분하지 않은 경우, 충돌을 피하기에는 고정 지형으로부터의 거리가 불충분하게 유지되는 경우이다. 물리적 장애가 부적절한 컨트롤을 유발할 수도 있지만 그 외에 고려해야 할 사항이 훨씬 많다.

안전에 시스템 이론을 적용하기 위해서는 현재 사용되는 모델을 확장하는 새로운 사고 인과 관계 모델(accident causality model)이 필요하다. STAMP(System-Theoretic Accident Model and Processes)는 직접적으로 관련된 일련의 실패 이벤트 또는 컴포넌트 실패를 다루는 전통적인 인과관계 모델을 확장하여 시스템 컴포넌트 간의 더 복잡한 프로세스 및 안전하지 않은 상호작용을 다룬다.[13] STAMP에서 사고는 물리적 시스템, 사람 및 시스템 간의 복잡한 상호작용으로 인해 발생한다. 안전은 실패 방지의 문제 보다는 동적 컨트롤 문제로 취급된다. STAMP 모델은 기존 원인을 누락시키지 않으면서(이벤트 체인 모델은 STAMP 모델의 부분 집합임) 더 많은 것들을 다루며, 실패 방지에 역점을 두는 것 시스템 동작에 대한 제약사항 강제에 역점을 두는 것으로 달라진다.

STAMP 사용의 장점은 다음과 같다:

- 매우 복잡한 시스템에 적용할 수 있다. 상향식(bottom-up)이 아닌 상위 수준의 추상화로부터 하향식(top-down)으로 진행되기 때문이다.
- 사고 및 다른 유형의 손실에 대한 원인 요소로서 소프트웨어, 사람, 조직, 안전 문화 등을 모두 포함하며, 따라서 그 요소들을 다르게 또는 별도로 취급할 필요가 없다.

[13] Nancy G. Leveson, *Engineering a Safer World,* MIT Press (2012), Cambridge MA 참고

In summary, the accident causality model and the information used to analyze why a loss occurred, will have a major impact on the causal factors identified and on the conclusions reached in an accident investigation. It's now time to introduce CAST, starting with its goals.

## Goals for an Improved Accident Analysis Approach

To summarize what has been presented so far**,** identifying what is labeled a "root cause" or focusing on blame unnecessarily limits what is considered in an accident investigation. Too many factors are missed and never fixed. It also limits the scope and effectiveness of the investigation as, after a loss, everyone tries to point fingers at someone else.

Instead, the goal of the causal analysis should be to learn from a loss in order to prevent future ones—not to find someone or even something to blame. Many of these people, usually low-level operators, have simply been caught up in a system where a loss was inevitable and that person was unlucky enough to be the one that triggered or was involved in the events for an accident that was "waiting to happen."

An accident analysis technique that maximizes learning from accidents and incidents should have the following goals:

1. Include all causes (optimize learning) and not focus on a few so-called "root" or "probable" causes.
2. Reduce hindsight bias.
3. Take a system's view of human behavior.
4. Provide a blame-free explanation of why the loss occurred; consider "why" and "how" rather than "who."
5. Use a comprehensive accident causality model that emphasizes why the controls that were created to prevent the particular type of loss were not effective in the case at hand and how to strengthen the safety control structure to prevent similar losses in the future.

CAST was created with these goals in mind and was developed and refined from experience gained over several decades of investigating complex accidents. The rest of this handbook will show you how to do a CAST analysis.

STAMP는 CAST의 기반이 되는 사고 인과관계 모델이다.

요약하면, 손실 발생의 원인 분석에 사용되는 사고 인과관계 모델과 정보는 원인 규명과 사고 조사의 결론에 큰 영향을 미칠 것이다. 이제 목표를 시작으로 CAST를 소개한다.

## 사고 분석 기법의 개선을 위한 목표

지금까지 제시된 내용을 요약해보면, "근본 원인(root cause)"이라고 레이블할 만한 것을 찾거나 책임에 초점을 맞추는 것은 사고 조사에서 고려되는 것들을 불필요하게 제한한다. 이 때문에 상당히 많은 요소들이 누락되거나 고쳐지지 않는다. 이는 또한 손실 발생 후 모두가 다른 누군가를 지적하게 하므로 조사의 범위와 효과를 제한시킨다.

원인 분석의 목표는 미래의 손실을 방지하기 위해 손실로부터 배우는 것이지, 비난할 누군가 또는 어떤 것을 찾는 것이 아니다. 보통 하위 수준의 운영자였던 사람들 중 다수가 손실이 불가피한 시스템에 붙잡혀 있었고, 운 나쁘게도 "발생이 예기된" 사고를 촉발시키거나 연루된 사람이 되었다.

사고와 사건으로부터의 학습을 극대화하는 사고 분석 기법은 다음과 같은 목표를 가져야 한다:

1. 모든 원인을 포함시키고(학습 최적화), 이른바 "근본(root)" 또는 "가능한(probable)" 몇 가지 원인에만 초점을 맞추지 않는다.
2. 사후 확신 편향(hindsight bias)을 줄인다.
3. 사람의 행동에 대해 시스템적 관점을 가진다.
4. 손실이 발생한 이유를 비난 없이 설명한다. "누구"보다는 "왜"와 "어떻게"를 고려한다.
5. 특정 유형의 손실을 방지하기 위해 만들어진 컨트롤이 그 상황에서 왜 효과적이지 않았는지를 강조하고, 향후 유사한 손실을 방지하기 위해 안전 컨트롤 스트럭처를 어떻게 강화할 것인지에 대한 포괄적인 사고 인과관계 모델을 사용한다.

CAST는 이러한 목표를 위해 만들어졌으며 수십 년 동안 복잡한 사고를 조사한 경험을 바탕으로 개발되고 개선되었다. 다음 장부터 CAST 수행 방법을 다루고자 한다.

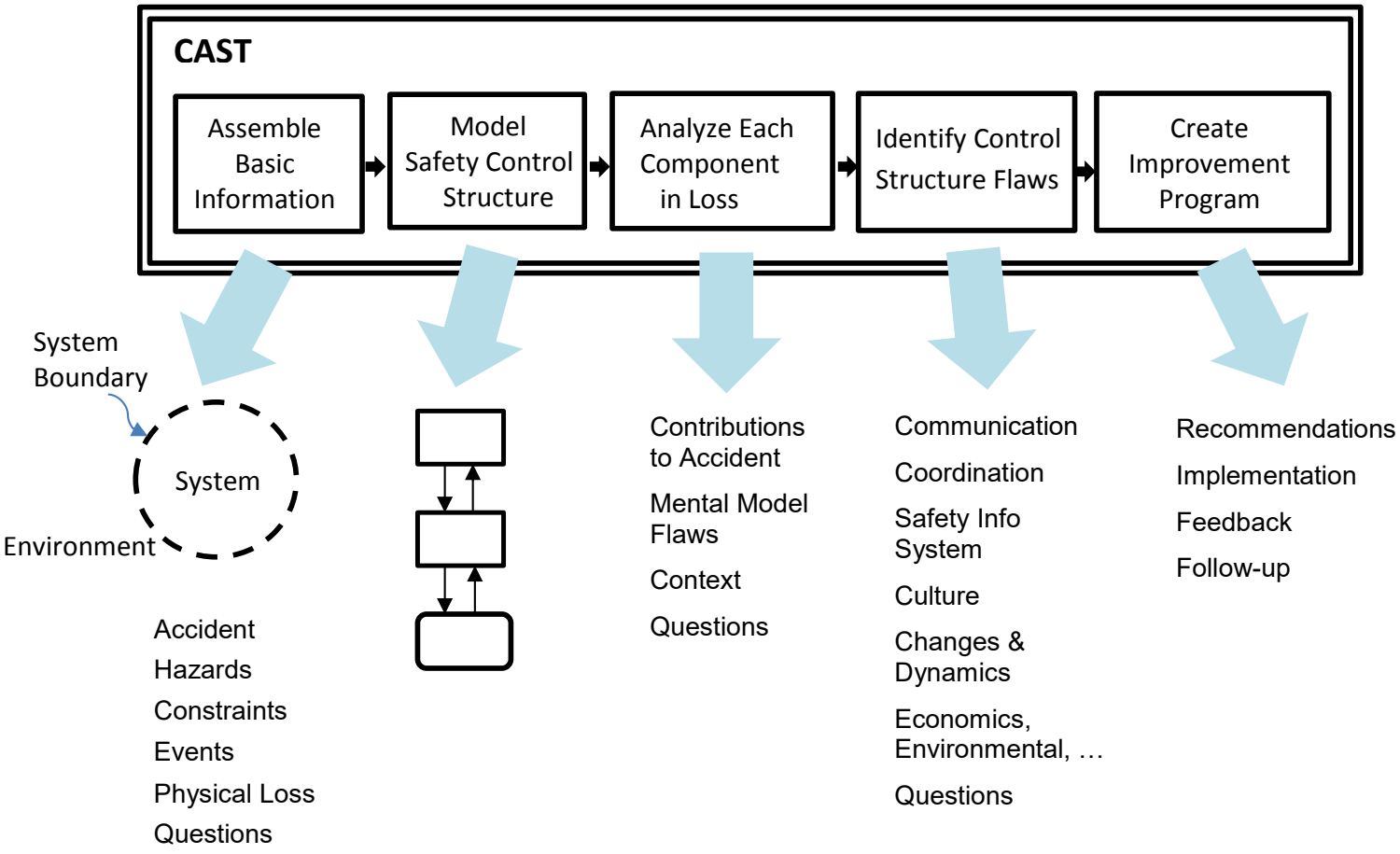
# Chapter 4: Performing a CAST Analysis

## Basic Components of CAST

CAST (Causal Analysis Based on Systems Theory) is a structured technique to analyze accident causality from a systems perspective.[14] CAST is an analysis method, not an investigation technique. But performing the CAST analysis as the investigation proceeds will assist in identifying what questions need to be answered and what information needs to be gathered during the investigation in order to create a comprehensive explanation as to why the loss occurred and to help formulate recommendations to prevent related accidents in the future.

Because the cause of an accident is defined in STAMP to be a safety control structure that did not prevent the loss, then the goal of the accident investigation is to identify why the safety control structure was unable to enforce the safety constraint that was violated and to determine what changes in the control structure are required to prevent a related loss in the future. In most cases, investigators will find that there was inadequate control provided at all levels of the safety control structure, not just the lower levels.

CAST has five parts:




[14] It is unfortunate that the same acronym is used for Commercial Aviation Safety Team. Both uses have existed for so long that there does not seem to be a simple solution. In this handbook, CAST is always used to mean Causal Analysis based on System Theory.

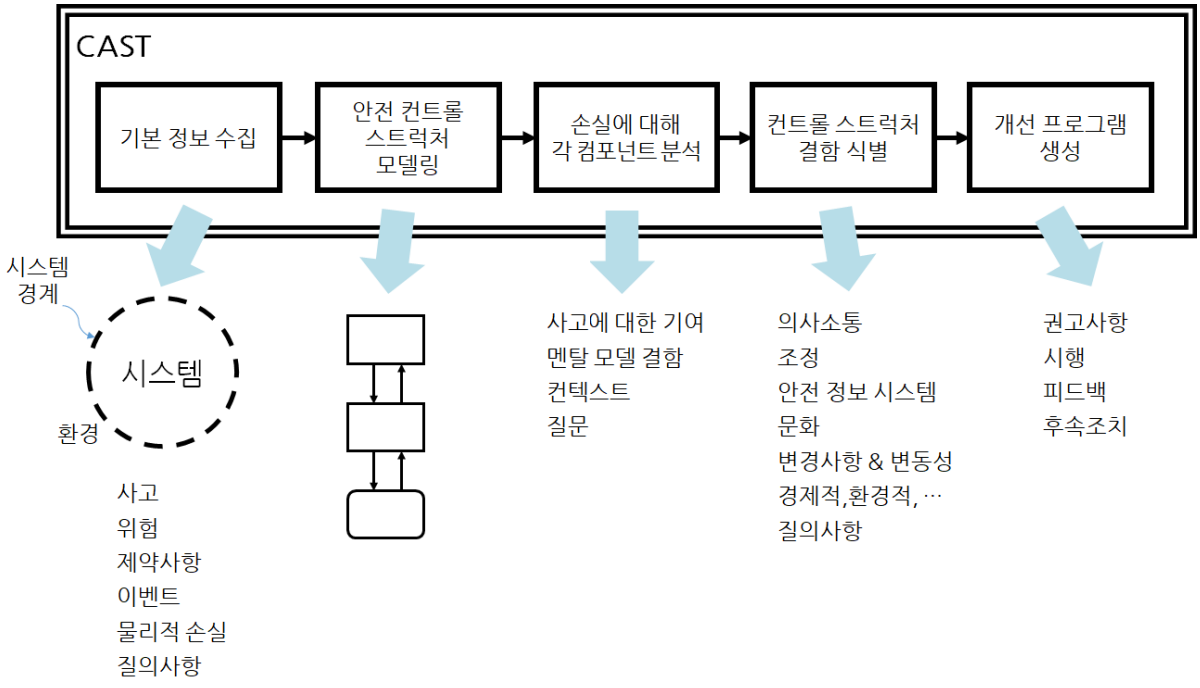
# 4장 : CAST 분석 수행

## CAST의 기본 구성요소

CAST(Causal Analysis Based on Systems Theory)는 시스템 관점에서 사고 인과관계를 분석하는 구조화된 기법이다.[14] CAST는 분석 방법이며 조사 기법은 아니다. 그러나 조사가 진행되는 과정에서 CAST 분석을 수행하면, 손실이 발생한 이유에 대한 포괄적인 설명에 도움이 되기 위해 그리고 향후 관련 사고 예방을 위한 권고안을 수립하기 위해 조사 과정에서 어떤 질문에 답해야 하는지, 어떤 정보가 수집되어야 하는지를 파악하는 데 도움이 될 것이다.

STAMP에서 사고의 원인은 손실을 방지하지 못한 안전 컨트롤 스트럭처로 정의되기 때문에 사고 조사의 목적은, 안전 컨트롤 스트럭처가 왜 위반된 안전 제약사항을 강제하지 못했는지를 파악하고 향후에 관련된 손실을 방지하기 위해 컨트롤 스트럭처에 어떤 변경이 필요한지를 결정하는 것이다. 대부분의 경우, 조사관은 낮은 레벨뿐만 아니라 모든 레벨의 안전 컨트롤 스트럭처에서 부적절한 컨트롤이 있었음을 발견할 것이다.

CAST는 5개의 파트로 구성되어 있다:




[14] 동일한 약어로 Commercial Aviation Safety Team이 있는 것은 유감이다. 두 가지 약어 모두 오랫동안 사용되어 왔기 때문에 간단한 해결책은 없는 것 같다. CAST는 이 핸드북에서 항상 시스템 이론에 기반한 원인 분석을 의미하는 데 사용된다.

### *Basic Components of a CAST Analysis*

1. *Collect the basic information to perform the analysis:*
   a. *Define the system involved and the boundary of the analysis,*
   b. *Describe the loss and hazardous state that led to it*
   c. *From the hazard, identify the system-level safety constraints required to prevent the hazard (the system safety requirements and constraints).*
   d. *Describe what happened (the events) without conclusions nor blame. Generate questions that need to be answered to explain why the events occurred.*
   e. *Analyze the physical loss in terms of the physical equipment and controls, the requirements on the physical design to prevent the hazard involved, the physical controls (emergency and safety equipment) included in the design to prevent this type of accident, failures and unsafe interactions leading to the hazard, missing or inadequate physical controls that might have prevented the accident, and any contextual factors that influenced the events.*

   *The goal of rest of analysis is to identify the limitations of the safety control structure that allowed the loss and how to strengthen it in the future.*
2. *Model the existing safety control structure for this type of hazard.*
3. *Examine the components of the control structure to determine why they were not effective in preventing the loss: Starting at the bottom of the control structure, show the role each component played in the accident and the explanation for their behavior (why they did what they did and why they thought it was the right thing to do at the time).*
4. *Identify flaws in the control structure as a whole (general systemic factors) that contributed to the loss. The systemic factors span the individual system control structure components.*
5. *Create recommendations for changes to the control structure to prevent a similar loss in the future. If appropriate, design a continuous improvement program for this hazard as part of your overall risk management program.*

These are not rigid steps or a straight-line process. Work on each of the parts may proceed throughout the investigation as deemed appropriate and practical, although the first two parts will provide the basic information for the later activities and probably need to be at least started before attempting the other parts. As more is learned during the investigation, analyses will be revisited and results changed or holes filled in.

Each step involves generating questions to answer later as more is learned. The questions will help the investigators determine what more needs to be learned to explain in depth why the loss occurred. The goal at the end of the investigation is to be able to answer all the questions or to determine that they are unanswerable. The answers to the questions will provide the “why’s” for the events.

A required format for recording the results of the analysis is not provided in this handbook. Different formats may be appropriate in different situations. Some examples are provided at the end of the chapter but you may find a better format for your purposes. In addition, some industries, such as aviation, have a required format and contents for the final investigation report, which may influence the format for the CAST analysis itself.

A running example analysis is used in this handbook to explain the CAST process. It is a real accident: an explosion of a chemical reactor and a fire on June 3, 2014 at the Shell Moerdijk plant in the Netherlands. The contents of the reactor were released into the wider environment, while sections of the reactor itself were blasted across 250 meters and other debris was later found 800 meters away.

*CAST 분석의 기본 구성요소*

1. *분석에 필요한 기초자료를 수집한다:*
   a. *관련된 시스템과 분석의 경계를 정의한다.*
   b. *손실 및 손실을 발생시킨 위험 상태를 설명한다.*
   c. *위험으로부터, 위험을 방지하는 데 필요한 시스템 수준의 안전 제약사항(시스템 안전 요구사항 및 제약사항)을 식별한다.*
   d. *판단이나 비난 없이 무슨 일(사건)이 일어났는지 설명한다. 왜 그런 일이 일어났는지 설명하기 위해 답변 받아야 할 질문들을 생성한다.*
   e. *물리적 장비와 컨트롤 측면의 물리적 손실, 관련된 위험을 예방하기 위한 물리적 설계 요구사항, 이러한 유형의 사고 예방을 위해 설계에 포함된 물리적 컨트롤(비상 및 안전 장비), 위험을 초래한 실패 및 안전하지 않은 상호작용, 사고를 예방할 수도 있었던 누락되었거나 부적절한 물리적 컨트롤, 이벤트에 영향을 미쳤던 모든 컨텍스트적 요인을 분석한다.*

   *나머지 분석의 목표는 손실을 허용하는 안전 컨트롤 스트럭처의 한계를 파악하고 향후 이를 강화하는 방법을 도출하는 것이다.*
2. *이러한 위험 유형에 대한 기존의 안전 컨트롤 스트럭처를 모델링한다.*
3. *컨트롤 스트럭처의 컴포넌트를 조사하여 손실 방지에 효과가 없었던 이유를 파악한다: 컨트롤 스트럭처의 가장 아래에서 시작하여 사고에서 각 컴포넌트가 수행한 역할과 동작에 대한 설명(그들이 한 일과 그 당시에 왜 옳다고 생각했는지)을 제시한다.*
4. *손실에 기여한 컨트롤 스트럭처의 결함을 전체의 관점(종합적인 시스템적 요인)에서 식별한다. 시스템적 요인은 시스템 컨트롤 스트럭처 컴포넌트 각각에 분포되어 있다.*
5. *향후 유사한 손실을 방지하기 위해 컨트롤 스트럭처에 대한 변경 권고사항을 작성한다. 가능하면 전체적인 리스크 관리 프로그램의 일부로서 이 위험에 대한 지속적인 개선 프로그램을 설계한다.*

각 단계가 엄격해야 하거나 절차를 순서대로 따라야 하는 것은 아니다. 처음 두 파트는 이후 활동에 대한 기본 정보를 제공하므로 적어도 다른 파트를 수행하기 전에 시작해야 하지만, 각 파트가 적절하고 현실적이라면 조사 전반에 걸쳐 진행될 수 있다. 조사 과정에서 더 많은 것을 알게 됨에 따라 분석이 재검토되고 결과가 바뀌거나 빈 곳이 채워진다.

이후 더 많은 것을 배우면서 각 단계에서 질문이 발생된다. 이 질문들은 조사관들이 손실 발생 이유를 심도 있게 설명하기 위해 무엇을 더 알아야 하는지 결정하는 데 도움이 될 것이다. 조사 막바지의 목표는 모든 질문에 대답하거나 일부 질문은 대답할 수 없는 질문이라고 판단하는 것이다. 질문에 대한 답은 발생된 이벤트에 대한 "이유(why's)"를 제공할 것이다.

이 핸드북에서는 분석 결과의 기록에 필요한 형식은 제공되지 않는다. 상황에 따라 다른 형식이 적절할 수 있다. 이 장의 마지막에 몇 가지 예시가 나와 있지만 목적에 따라 더 나은 형식을 활용해도 된다. 또한 항공과 같은 일부 산업에서는 최종 조사 보고서에 필요한 형식과 내용이 정해져 있어 CAST 분석 자체의 형식에 영향을 줄 수 있다.

이 핸드북에서는 CAST 프로세스 설명을 위해 연속된 사례 분석을 사용한다. 이 예제는 실제 사고이다: 2014년 6월 3일 네덜란드의 쉘 뫼르딕 플랜트의 화학 반응로에 화재와 폭발이 발생했다. 반응로의 내용물이 외부 환경으로 방출되었고, 반응로 자체는 250미터에 걸쳐 폭파되었으며 일부 파편은 나중에 800미터 떨어진 곳에서 발견되었다. 20km 떨어진 곳에서도 폭발음이 들렸다. 폭발하는 반응로

The explosion could be heard 20 kilometers away. Two people working opposite the exploding reactor were hit by the pressure wave of the explosion and the hot and burning catalyst pellets that were flying around. A large, raging fire occurred, generating considerable amounts of smoke.



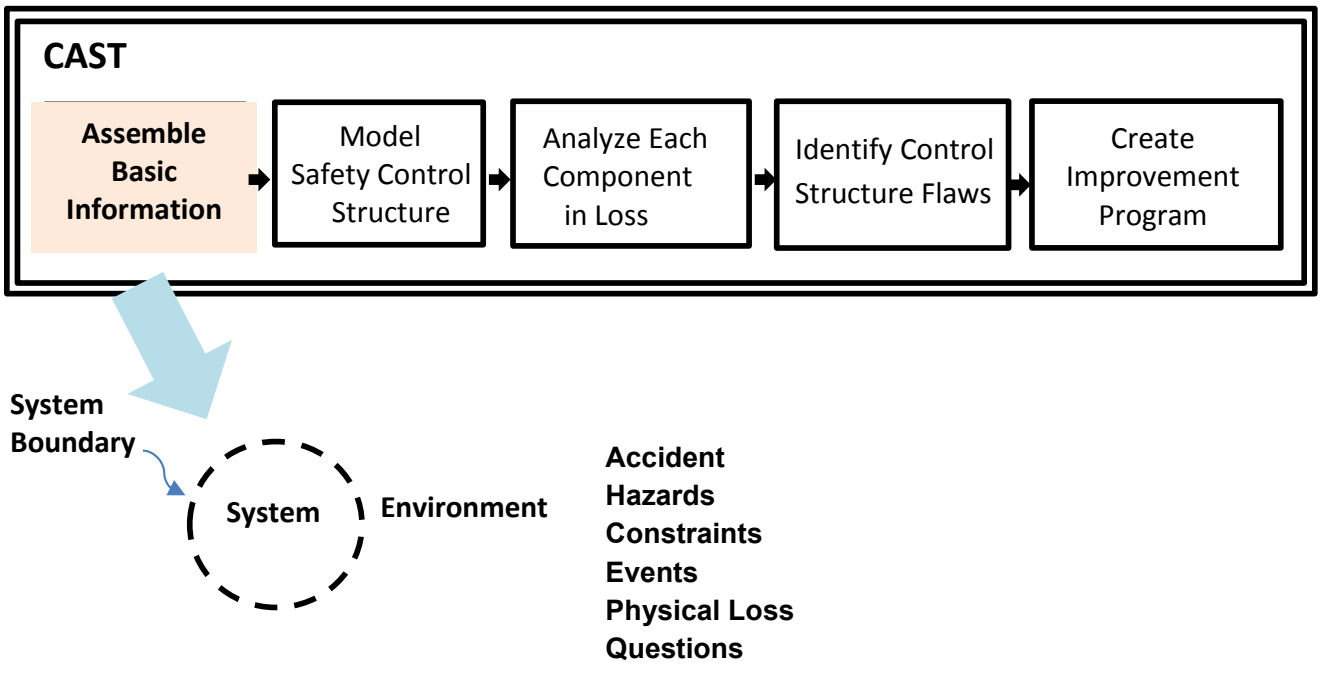
**Figure 12**: The Shell Moerdijk Explosion

Links to other online examples of real CAST analyses on a large variety of accidents, including the running example used here, is provided in Appendix A.

The complete CAST analysis for this accident is too large to include in this handbook but can be accessed online through the link provided in Appendix A. Technical information about the chemical process that goes beyond what is needed to understand the CAST example is provided in Appendix B, along with a summary of the full CAST analysis results.

The rest of this chapter describes how each of the CAST process steps is performed on the example accident. I recommend that you take an accident with which you are familiar and go through the CAST steps yourself on that accident as you read the explanation and the examples.

## Assembling the Foundational Information



맞은편에서 일하는 두 사람은 폭발의 압력파와 주변에 날아다니는 뜨겁고 불타는 촉매제 펠릿에 맞았다. 크고 격렬한 화재가 발생하면서 상당한 양의 연기가 발생했다.



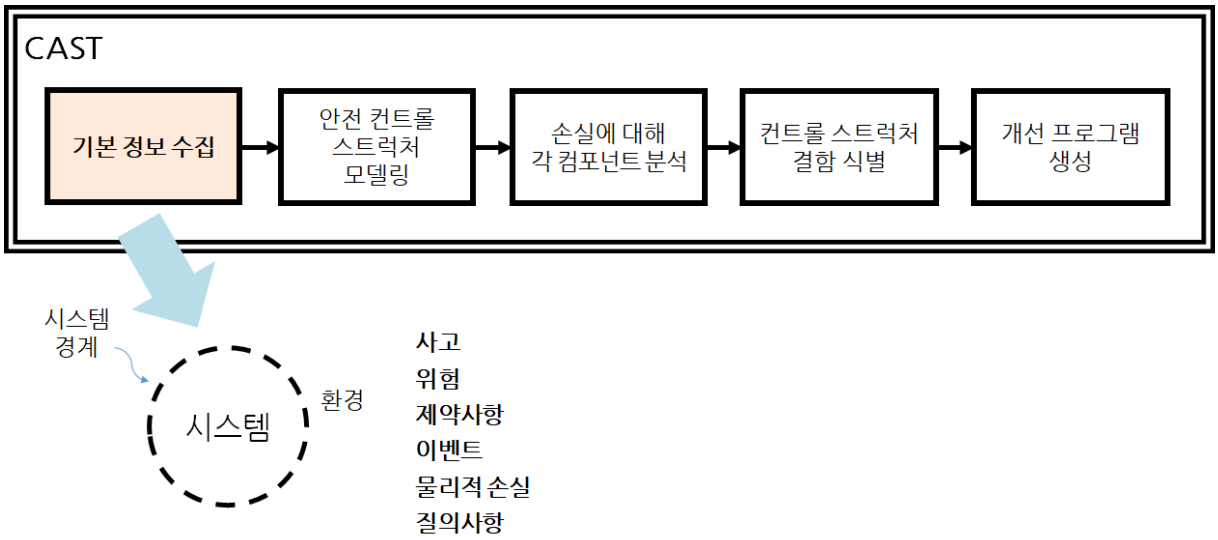
그림 12: 쉘 뫼르딕 플랜트 폭발

여기에 사용된 예제를 포함하여, 다양한 사고에 대한 실제 CAST 분석 예제에 대한 링크를 부록 A에 수록하였다.

이 사고에 대한 완전한 CAST 분석을 이 핸드북에 포함하기에는 너무 방대하며 부록 A에 제공된 링크를 통해 온라인으로 확인할 수 있다. 부록 B에서는 CAST 예제 이해에 필요한 화학 공정 및 그 이상의 기술 정보와 전체 CAST 분석 결과 요약을 수록하였다.

이 장의 나머지 부분에서는 위 사고 사례에서 각 CAST 프로세스 단계를 수행하는 방법을 설명한다. 필자는 당신이 겪은 사고와 유사한 사고 사례를 골라 설명과 예시를 읽으면서 그 사고에 대한 CAST 단계를 직접 수행하는 것을 추천한다.

## 기본 정보 수집



*1. Collect the basic information to perform the analysis:*
   *a. Define the system involved and the boundary of the analysis,*
   *b. Describe the loss and hazardous state that led to it*
   *c. From the hazard, identify the system-level safety constraints required to prevent the hazard (the system safety requirements and constraints).*
   *d. Describe what happened (the events) without conclusions nor blame. Generate questions that need to be answered to explain why the events occurred.*
   *e. Analyze the physical loss in terms of the physical equipment and controls, the requirements on the physical design to prevent the hazard involved, the physical controls (emergency and safety equipment) included in the design to prevent this type of accident, failures and unsafe interactions leading to the hazard, missing or inadequate physical controls that might have prevented the accident, and any contextual factors that influenced the events.*

*The goal of rest of analysis is to identify the limitations of the safety control structure that allowed the loss and how to strengthen it in the future.*

The first step is simply to gather basic information about what happened and to identify the goals for the analysis. The system hazard that occurred and the safety constraint violated are first identified. While seemingly simple and obvious, the hazard(s) and safety constraint(s) are important in identifying the controls included in the safety control structure in order to prevent this hazard and enforce the constraints. Starting from all constraints and controls is too inefficient.

We start by identifying the boundaries of the system of concern. In the Shell Moerdijk accident, the system analyzed is the chemical plant, its equipment, and the workers in the plant as well as the public in the area around the plant. The loss involved an explosion of Unit 4800 during startup after a maintenance stop. More details are included in Appendix B.

Next, the hazards that led to the loss and the constraints that must be satisfied in the design and operation of the system are identified.

*System Hazard 1*: Exposure of the public or workers to toxic chemicals.

Safety Constraints:

1. Workers and the public must not be exposed to potentially harmful chemicals.
2. Measures must be taken to reduce exposure if it occurs.
3. Means must be available, effective, and used to treat exposed individuals inside or outside the plant.

*System Hazard 2*: Explosion (uncontrolled release of energy) and/or fire.

Safety Constraints:

1. Chemicals must be under positive control at all times, i.e., runaway reactions must be prevented.
2. Warnings and other measures must be available to protect workers in the plant and to minimize losses to the outside community.
3. Means must be available, effective, and used to respond to explosions or fires inside or outside the plant.

*1. 분석에 필요한 기본 정보를 수집한다:*
   *a. 관련된 시스템과 분석의 경계를 정의한다.*
   *b. 손실 및 손실을 발생시킨 위험 상태를 설명한다.*
   *c. 위험으로부터, 위험을 방지하는 데 필요한 시스템 수준의 안전 제약사항(시스템 안전 요구사항 및 제약사항)을 식별한다.*
   *d. 판단이나 비난 없이 무슨 일(사건)이 일어났는지 설명한다. 왜 그런 일이 일어났는지 설명하기 위해 답변 받아야 할 질문들을 생성한다.*
   *e. 물리적 장비와 컨트롤 측면의 물리적 손실, 관련된 위험을 예방하기 위한 물리적 설계 요구사항, 이러한 유형의 사고 예방을 위해 설계에 포함된 물리적 컨트롤(비상 및 안전 장비), 위험을 초래한 실패 및 안전하지 않은 상호작용, 사고를 예방할 수도 있었던 누락되었거나 부적절한 물리적 컨트롤, 이벤트에 영향을 미쳤던 모든 컨텍스트적 요인을 분석한다.*

*나머지 분석의 목표는 손실을 허용하는 안전 컨트롤 스트럭처의 한계를 파악하고 향후 이를 강화하는 방법을 도출하는 것이다.*

첫 번째 단계는 발생한 사건에 대한 기본적인 정보를 수집하고 분석의 목표를 확인하는 것이다. 먼저, 발생된 시스템 위험과 위반된 안전 제약사항을 파악한다. 겉보기에는 단순하고 당연해 보이지만 위험을 예방하고 제약사항을 강제하기 위해서는 컨트롤 스트럭처에 포함된 컨트롤을 식별할 때, 발생한 위험(들)과 위반된 안전 제약사항(들)을 파악하는 것이 중요하다. 모든 제약사항과 컨트롤에서부터 조사를 시작하는 것은 너무나 비효율적이기 때문이다.

우선, 관련된 시스템의 경계를 파악하는 것부터 시작한다. 쉘 뫼르딕 사고에서 분석된 시스템에는 화학 플랜트, 장비 및 작업자뿐만 아니라 플랜트 주변 지역의 일반인이 포함되었다. 유지 보수 중지 후 기동 과정에서 Unit 4800의 폭발로 인해 손실이 발생했다. 자세한 내용은 부록 B에 있다.

다음으로, 손실로 이어진 위험과 시스템의 설계 및 운영에서 충족되어야 하는 제약사항을 파악한다.

*시스템 위험 1*: 일반인 또는 작업자가 독성 화학 물질에 노출됨

안전 제약사항:

1. 작업자와 일반인이 유해한 화학물질에 노출되어서는 안 된다.
2. 만일 노출되는 일이 발생하면, 노출을 줄이기 위한 대책을 수립해야 한다.
3. 화학 물질에 노출된 플랜트 내부 또는 외부의 사람들을 치료할 수 있는 수단은 가용하고 효과적이어야 한다.

*시스템 위험 2*: 폭발(컨트롤되지 않은 에너지 유출) 및/또는 화재가 발생함

안전 제약사항:

1. 화학 물질은 항상 정상적인 상태 내에서 컨트롤 되어야 한다. 즉, 폭주 반응(runaway reactions)이 예방되어야 한다.
2. 플랜트 작업자를 보호하고 외부 지역사회에 대한 손실을 최소화하기 위해 경고나 기타 조치를 취해야 한다.
3. 플랜트 내부 또는 외부의 폭발이나 화재에 대응하기 위한 수단은 가용하고 효과적이어야 한다.

In this case, there were two hazards that occurred. The constraints include the concerns of the investigation and the safety control structure to be considered that extend beyond the boundaries of the plant itself and, indeed, beyond the responsibilities of Shell. For example, responsibility for public (community) health is not normally the sole responsibility of the owners of the chemical plant itself, although they may by law be required to participate.

Deriving the safety constraints from the hazard is rather obvious, except perhaps for the inclusion of constraints to handle the case where the hazard is not avoided. In System Hazard 1 for the chemical plant (*Exposure of the public or workers to toxic chemicals*), the first safety constraint is simply a translation of the hazard to a goal statement, i.e., workers and the public must not be exposed to potentially harmful chemicals.

The second and the third are more easily missed. There is always a possibility that the safety constraint is not enforced. In that case, the hazard cannot be avoided, but it often can be mitigated and any potential harm reduced if the hazard occurs. That is the purpose of the second and third safety constraints, which require that the designers and controllers of the system and of the system's environment respond appropriately (1) to mitigate the impacts of the hazard as much as possible if the hazard does occur and (2) to minimize any potential losses if the hazard's impact cannot be totally mitigated.

Specifying the hazard itself is a bit trickier. In Chapter 1, a hazard is defined as something that has to be under the control of or within the boundaries of the system being designed. That argument is not repeated here. In engineering, designers and operators can only prevent something that they have control over. In addition, design and operations have to be performed considering the worst-case environment, not the expected or average case.

A common mistake is to state the hazard with respect to a system component and not as a statement about the system as a whole. Failure or unsafe behavior of a system component is not a system hazard—it is a cause of a hazard. Causes will be identified later in the CAST process. By starting at the system level and later generating the causes of the system hazards, you are much less likely to omit whole pieces of the puzzle in your causal analysis. It will also be easier to identify when causes are missing.

Here are some examples of proper system hazards and some that are not:

System hazard: The aircraft stalls and does not have adequate airspeed to provide lift.

Non-system-hazard: The engines do not provide enough propulsion to remain airborne.

Non-system- hazard: The pilots do not keep the angle-of-attack down to prevent or respond to a stall.

System hazard: The automobile violates minimum separation requirements from the car ahead

Non-system-hazard: The driver maneuvers the car in a way that violates minimum separation

Non-system-hazard: The automation does not slow the car adequately to avoid violating minimum separation from the car ahead

Non-system-hazard: Brake failure.

System hazard: Explosion and fire in a chemical plant

Non-system-hazard: Failure of the pressure release valve

Non-system-hazard: Over-pressurization of the reactor

Non-system-hazard: Operators not maintaining control over the reactor pressure

Non-system-hazard: Inappropriate reactor design for the chemical being produced.

이 사례에서는 두 가지 위험이 발생했다. 제약사항에는 조사와 안전 컨트롤 스트럭쳐의 중요한 것들이 포함되어 있으며, 이는 플랜트 자체의 경계를 넘어서며 실제로 쉘의 책임을 넘어선다. 예를 들어 공공(지역사회) 건강에 대한 책임에 대해 법적으로 참여를 요구할 수 있지만 이는 일반적으로 화학 플랜트 소유자의 단독 책임은 아니다.

제약사항은 피할 수 없는 위험을 다루는 경우를 제외하고는 위험을 토대로 도출하는 것이 확실하다. 화학 플랜트의 시스템 위험 1*(일반인 또는 작업자가 독성 화학물질에 노출됨)*의 첫 번째 안전 제약사항은 단순히 위험을 목표 형태의 문장으로 바꾸면 된다. 즉, "작업자와 일반인은 잠재적으로 유해한 화학 물질에 노출되어서는 안 된다."와 같이 작성하면 된다.

두 번째와 세 번째 안전 제약사항은 좀 더 간과하기가 쉽다. 안전 제약사항이 시행되지 않을 가능성은 항상 존재한다. 이 경우 위험을 피할 수는 없지만 위험이 발생할 경우 위험을 완화하고 잠재적인 피해를 줄일 수는 있다. 그것이 두 번째 및 세 번째 안전 제약사항의 목적이다. 즉, 시스템 및 시스템 환경의 설계자와 컨트롤러는 (1)위험 발생 시 위험의 영향을 최대한 완화하기 위해 적절하게 대응해야 하며 (2)위험의 영향을 완전히 완화할 수 없는 경우에는 잠재적 손실을 최소화해야 한다.

위험 자체를 명세하는 것은 다소 까다로운 일이다. 1장에서 위험이란, 설계 중인 시스템의 범위 내 또는 컨트롤 하에 있어야 하는 것이라고 정의한 바 있다. 여기서 이 내용을 반복하지는 않겠다. 엔지니어링에 있어서 설계자와 운영자는 자신이 컨트롤 할 수 있는 것들에 대해서만 방지할 수 있다. 또한, 설계자나 운영자는 예상되거나 평균적인 경우가 아닌 최악의 경우를 고려하여 설계하거나 운영해야 한다.

일반적으로 많이 하는 실수는 위험을 시스템 전체 측면에서가 아니라 시스템 구성요소 측면에서 정의하는 것이다. 시스템 구성요소의 실패나 안전하지 않은 동작(unsafe behavior)은 시스템 위험이 아니다 – 이것은 위험의 원인이다. 원인은 CAST 프로세스 뒷부분에서 다루게 될 것이다. 시스템 수준에서 위험을 식별하고 나중에 시스템 위험의 원인을 파악하면 원인 분석과정에서 퍼즐의 전체 조각을 빠뜨릴 가능성이 훨씬 줄어든다. 또한 원인이 누락될 때 이를 파악하는 것도 더 쉽다.

다음은 몇 가지 적절한 시스템 위험의 예와 그렇지 않은 예이다.

시스템 위험: 항공기가 실속(失速, stall) 상태가 되고 양력(lift)를 제공하기 위한 대기속도(airspeed)가 부족하다.
- 시스템 위험이 아닌 것: 비행(airborne)을 유지하기 위한 엔진의 추진력이 부족하다.
- 시스템 위험이 아닌 것: 조종사가 실속을 방지 혹은 대응하기 위해 받음각(angle-of-attack)을 다운시키지 않는다.

시스템 위험: 자동차가 전방 차량과의 최소 이격 거리 요구사항을 위반한다.
- 시스템 위험이 아닌 것: 운전자가 최소 이격 거리를 위반하며 자동차를 운전한다.
- 시스템 위험이 아닌 것: 자동차가 전방 차량과의 최소 이격 거리를 위반하지 않을 정도로 충분하게 속도를 늦추지 않는다.
- 시스템 위험이 아닌 것: 브레이크 고장

시스템 위험: 화학 플랜트에서의 폭발 및 화재
- 시스템 위험이 아닌 것: 압력 방출 밸브의 고장
- 시스템 위험이 아닌 것: 반응로의 과압
- 시스템 위험이 아닌 것: 작업자가 반응로 압력에 대한 컨트롤을 유지하지 않는 것
- 시스템 위험이 아닌 것: 화학 물질 생산을 위한 반응로의 부적절한 설계

Why are these limits on the specification of hazards being imposed? Consider the last example of an incorrect system-level hazard: "inappropriate reactor design for the chemical being produced." The problem is that it ignores the question of whether that chemical should have been produced at all or whether it should have been produced under the larger plant conditions that existed at the time. Instead, it focuses on design of the reactor and not on the operations of the other components of the plant, which may have contributed to the loss. It ignores management decisions that may have played a role. Instead, it immediately focuses the investigation down to the physical design level of part of the system, that is, the reactor design itself.

Remember, our goal is not just to find an explanation for the events but to identify the most comprehensive explanation and *all* contributions to the loss in order to maximize learning and to prevent as many future losses as possible. Focusing on the behavior of one component will lead to missing the contributions of other system components and the interactions among multiple components, like the car, the driver, the design of the interface between the car and the driver, etc. Rarely, if ever, is only one system component involved in a loss; focusing too narrowly leads to missing important information.

At this point, the events can be delineated if desired. Given the limited usefulness of the chain of events in investigating a loss, generating it is not required to complete a CAST analysis. It can, in fact, divert attention away from where it should be directed. Focusing on events alone does not provide the information necessary to determine why the events occurred, which is the goal of the CAST analysis.

While not required to start a CAST analysis, identifying the proximate events preceding the loss may sometimes be useful in starting the process of generating questions that need to be answered in the accident investigation and causal analysis. Table 1 shows the primary proximate events leading up to and following the explosion at Shell Moerdijk and some questions they raise that any accident analysis should answer. Once again, the goal is to identify ways to prevent such accidents in the future, not to find someone or something to blame.

Remember that the goal of listing the events is NOT to select one or several to identify as the cause of the loss. Instead the goal is to generate questions for the investigation that will be used in the overall causal analysis. Do not use blame-laden words such as the operators *failed* to … or "should have" in describing the events. These imply conclusions and blame. Simply describe what the hardware or operators did or did not do.

**Table 1: Proximal Events Leading up to the Shell Moerdijk Loss**

| ID | Event | Example Questions Raised |
|---|---|---|
| 1. | The plant had been shut down for a short, scheduled maintenance stop (called a pit stop) to replace the catalyst pellets and was being restarted at the time of the explosion | *Accidents usually occur after some type of change (planned or unplanned). The change may commonly involve a shutdown, a startup, or maintenance (including a workaround or temporary "fix"). Was there an MOC (Management of Change) policy for the plant and the company? If so, was it followed? If it was not followed, then why not? If it was followed, then why was it not effective?* |
| 2. | One of the restart procedures is to warm up the reactors with ethylbenzene. During the warming (reheating) process, uncontrolled | *Why were the reactions unforeseen? Were they foreseeable? Were there precursors that might have been used to foresee the reactions? Did* |

위험을 명세할 때 이와 같은 제한을 두는 이유는 무엇일까? 시스템 수준 위험에 대한 마지막 잘못된 예시를 생각해보자: "화학 물질 생산을 위한 반응로의 부적절한 설계", 이 예시의 문제는 화학 물질이 전혀 생산되지 않았어야 했는지 또는 당시 존재했던 더 큰 플랜트 조건 하에서 생산되었어야 했는지에 대한 질문을 고려하지 않는다는 것이다. 대신 이 예시는, 반응로 설계에만 집중하고 손실에 영향을 미칠 수 있는 플랜트에서의 다른 구성요소의 운영에 대해서는 집중하지 않는다. 이는 역할을 수행했을 수 있는 관리상의 결정을 무시한 것이다. 대신, 시스템 일부, 즉 원자로 설계 자체의 물리적 설계 수준 조사에 초점을 맞추게 한다.

우리의 목표는 이벤트에 대해 설명을 하는 것이 아니라 학습을 극대화하고 가능한 한 많은 미래의 손실을 방지하기 위해 손실에 대한 가장 포괄적인 설명과 모든 기여요소들을 확인하는 것임을 기억하기 바란다. 한 컴포넌트의 동작에만 초점을 맞추면 다른 시스템 컴포넌트의 기여 요소가 누락되고 자동차, 운전자, 자동차와 운전자 사이의 인터페이스 설계 등과 같은 여러 컴포넌트 간의 상호작용이 누락될 것이다. 손실이 한 가지 시스템 컴포넌트에만 관련된다는 것은 극히 드문 일이다; 너무 좁은 범위에 대해 집중하면 중요한 정보가 누락된다.

이 때, 원한다면 이벤트에 대해 상세하게 기술할 수 있다. 손실 조사에 있어 이벤트 체인의 유용성이 제한적임을 감안한다면, CAST 분석을 완료하기 위해 이벤트 체인을 생성할 필요는 없다. 사실 이벤트 체인은 조사 시 향해야 하는 곳으로부터 주의를 멀어지게 할 수도 있다. 이벤트에만 집중하는 것은 이벤트가 발생한 이유 파악에 필요한 정보를 제공하지 못하며 이벤트 발생 이유를 파악하는 것이 CAST의 목표이다.

CAST 분석을 시작하기 위해 필요한 것은 아니지만, 손실 이전에 발생한 가장 근접한 이벤트(proximate events)를 파악하는 것은 사고 조사와 원인 분석에서 답변되어야 하는 질문의 생성 과정을 시작하는 데 유용하다. 표 1은 쉘 뫼르딕 폭발 전후의 주요한 근접 이벤트들과 사고 분석을 통해 답변해야 할 몇 가지 질문들을 보여준다. 다시 말해, 목표는 비난할 대상이나 그 무언가를 찾는 것이 아니며 미래에 일어날지도 모르는 이러한 사고를 예방할 수 있는 방법을 찾는 것이다.

이벤트 나열의 목표는 손실 원인을 식별하기 위해 하나 또는 여러 개의 이벤트를 선택하는 것이 아님을 기억하기 바란다. 대신 전반적인 원인 분석에서 조사를 위해 사용할 질문을 만들어내는 것이 목표이다. 이벤트를 설명할 때 운영자가 *실패했다*거나 "했어야만 했다"와 같이 비난 가득한 단어를 사용해서는 안 된다. 이런 문구는 판단과 비난을 내포한다. 단순히 하드웨어나 운영자가 무엇을 했는지, 무엇을 하지 않았는지에 대해 설명하면 된다.

**표 1 : 쉘 뫼르딕 손실로 이어지는 주요 이벤트**

| ID | 이벤트 | 제기된 질문 예제 |
|---|---|---|
| 1 | 플랜트는 촉매제 펠릿을 교체하기 위해 예정된 유지보수를 위한 짧은 정지(pit stop이라고 함)를 위해 셧다운 되었고, 폭발 당시에 재가동 중이었다. | *사고는 보통 어떤 유형의 변경(계획되거나 계획되지 않은) 이후에 발생한다. 변경에는 일반적으로 종료, 구동 또는 유지보수(임시방편 또는 일시적인 "수정" 포함)가 포함될 수 있다. 플랜트와 회사에 대한 변경관리 (Management of change) 정책이 있었는가? 만약 그렇다면, 그것을 따랐는가? 따르지 않았다면 그 이유는 무엇인가? 만일 정책을 따랐다면, 왜 효과가 없었을까?* |
| 2 | 재가동 절차 중 하나는 에틸벤젠으로 반응로를 데우는 것이다. 가열(재가열) 과 | *왜 이런 결과들을 예상하지 못했던 것일까? 이런 결과들은 예견될 수 있었을까? 결과 예측에 활용할* |

| | | |
|---|---|---|
| | energy was released and unforeseen chemical reactions occurred between the warming up liquid (ethylbenzene) and the catalyst pellets that were used. | *the operators detect these reactions before the explosion? If not, then why not? If they did, why did they not do anything about controlling them?* |
| 3 | The reactions caused gas formation and increased pressure in the reactors. | *Did the design account for the possibility of this increased pressure? If not, why not? Was this risk assessed at the design stage?* |
| 4 | An automatic protection system was triggered that was designed to prevent liquid from entering the exhaust gas system (flare). But preventing the liquids from entering the flare also prevented the gases in the system from being discharged, increasing pressure in the reactor. | *Did the operators notice this? Was it detectable? Why did they not respond? This seems like a predictable design flaw. Was the unsafe interaction between the two requirements (preventing liquid from entering the flare and the need to discharge gases to the flare) identified in the design or hazard analysis efforts? If so, why was it not handled in the design or in operational procedures? If it was not identified, why not?* |
| 5 | Continued warming up of the reactors caused more chemical reactions to occur between the ethylbenzene and the catalyst pellets, causing more gas formation and increasing pressure in the reactor. | *Why wasn't the increasing pressure detected and handled? If there were alerts, why did they not result in effective action to handle the increasing pressure? If there were automatic overpressurization control devices (e.g., relief valves), why were they not effective? If there were not automatic devices, then why not? Was it not feasible to provide them?* |
| 6 | The pressure rose so fast that it could no longer be controlled by the pressure relief devices, and the reactor exploded due to high pressure and the separation vessel collapsed and exploded. | *Was it not possible to provide more effective pressure relief? If it was possible, why was it not provided? Was this type of pressure increase anticipated? If it was anticipated, then why was it not handled in the design or operational procedures? If it was not anticipated, why not?* |
| 7 | The contents of the reactor and its associated separation vessel were released into the wider environment. Sections of the reactor were blasted across 250 meters while other debris was later found 800 meters away. The explosion could be heard 20 kilometers away. | *Was there any way to contain the contents within some controlled area (barrier), at least the catalyst pellets?* |
| 8 | Two people working opposite Unit 4800 at the time of the explosion were hit by the pressure wave of the explosion and the hot and burning catalyst pellets that were flying around. | *Why was the area around the reactor not isolated during a potentially hazardous operation? Why was there no protection against catalyst pellets flying around?* |
| 9 | A large, raging local fire occurred, generating considerable amounts of smoke. | |

| ID | 이벤트 | 제기된 질문 예제 |
|---|---|---|
| | 정에서 제어되지 않은 에너지가 방출되었고 가열액(에틸벤젠)과 사용된 촉매제 펠릿 사이에 예기치 않은 화학 반응이 일어났다. | *수 있는 전조현상(precusor)이 있었는가? 운영자들은 폭발 전에 이러한 반응을 감지했는가? 그렇지 않다면, 왜 감지하지 못했는가? 만약 감지했다면, 왜 그것들을 통제하기 위해 아무것도 하지 않았는가?* |
| 3 | 이 반응으로 가스가 발생했고 반응로의 압력이 증가하였다. | *설계 시 이러한 압력 증가의 가능성을 고려하였는가? 그렇지 않다면, 그 이유는 무엇인가? 이 리스크는 설계 단계에서 평가되었는가?* |
| 4 | 액체가 배기가스 시스템(플레어)으로 유입되는 것을 방지하기 위해 설계된 자동 보호 시스템이 작동되었다. 그러나 액체가 플레어에 들어가는 것을 방지한 것으로 인해 시스템의 가스가 배출되지 않아 반응로의 압력이 더욱 증가하였다. | *운영자들이 이 상황을 인지했는가? 감지할 수 있었는가? 운영자들은 왜 대응하지 않았는가? 이것은 설계상의 예측 가능한 결함으로 보인다. 설계 또는 위험 분석 시 두 가지 요구사항(액체가 플레어에 유입되는 것과 플레어로 가스를 배출하는 것) 간의 안전하지 않은 상호작용이 식별되었는가? 만약 그렇다면 왜 설계나 운영 절차에서 다루지 않았는가? 만약 그것이 확인되지 않았다면, 왜 그러했는가?* |
| 5 | 반응로의 지속적인 온도 상승은 에틸벤젠과 촉매제 펠릿 사이에 더 많은 화학 반응을 일으켰고 이로 인해 발생한 많은 기체는 반응로의 압력을 증가시켰다. | *증가하는 압력이 감지되지 못하고 처리되지 못한 이유는 무엇인가? 경고 알람이 발생했다면, 왜 증가하는 압력을 처리하기 위해 효과적인 조치를 취하지 않았는가? 자동 과압제어장치(예: 방출밸브)가 있었다면 왜 효과가 없었는가? 자동 장치가 존재하지 않았다면, 왜 없었는가? 자동 장치를 제공하는 것이 실현 불가능한 것이었는가?* |
| 6 | 압력 상승 속도가 너무 빨라 더 이상 감압장치로 컨트롤 할 수 없었고, 반응로가 고압으로 인해 폭발했으며 분리용기가 붕괴되고 폭발했다. | *보다 효과적으로 압력을 완화할 수 없었는가? 만약 가능했다면, 왜 이루어지지 않았는가? 이러 식의 압력 증가를 예상하였는가? 만약 예상했다면, 설계나 운영 절차에서 처리되지 않은 이유는 무엇인가? 예상하지 못했다면, 그 이유는 무엇인가?* |
| 7 | 반응로와 그와 관련 분리 용기의 내용물은 넓은 범위의 환경에 걸쳐 유출되었다. 반응로의 섹션들이 250미터에 걸쳐 파괴되었고 파편들이 800미터 떨어진 곳에서 발견되었다. 폭발음이 20km 밖에서도 들렸다. | *최소한 촉매제 펠릿과 같은 내용물을 통제된 영역(배리어) 내에 담을 수 있는 방법이 있었는가?* |
| 8 | 폭발 당시 Unit 4800 맞은편에서 작업하던 두 사람이 폭발 압력파와 비산하는 뜨겁고 불타는 촉매제 펠릿에 맞았다. | *위험 가능성이 있는 작업을 하는 동안 반응로 주변 지역이 격리되지 않은 이유는 무엇인가? 왜 촉매제 펠릿이 주변을 날아다니는 것에 대한 보호조치가 없었을까?* |
| 9 | 크고 격렬한 국지적 화재가 발생했고 상당한 양의 연기가 발생했다. | |

10 Community firefighting, healthcare, crisis management, and crisis communications were initiated.

Notice that the word "failed" does not appear anywhere in the events description (and will not appear anywhere in the CAST analysis unless a physical component failure occurred). Nor are hindsight bias statements made such as "the operators should have …." It is way too early to start making judgments and conclusions (which should be avoided even later). In addition, the questions identified in this early part of the analysis are very general. As more is learned, these questions will be refined and the answers will generate many more questions. At the end, the goal is to answer all the questions or to determine that they cannot be answered. The answers together will provide an in-depth understanding of why this accident occurred and why the controls and protection devices did not mitigate the effects of the events.

The example event chain provided here is far from "complete" (whatever that might mean because more events could always be added). In fact, their completeness will have little impact on the results of the CAST analysis. The questions that need to be answered will be generated later if not here. The event chain simply can provide a starting place if one is not obvious. Again, starting with an event chain is not strictly necessary when doing a CAST analysis.

**SUGGESTED EXERCISE**: Take an accident with which you are familiar or for which you have access to a detailed description of what happened. Write down the major events. The list need not be complete; this is only a starting point. Create questions associated with the events that need to be answered to understand why the events occurred. Your questions will again almost surely not be complete unless the accident is very simple. The questions you create simply form a starting point in your thinking. Many more will be created (and hopefully answered) as you go through the CAST process.

## Understanding What Happened in the Controlled Process

Identifying "why" something occurred requires first knowing "what" occurred. Physical injury or losses necessarily involve a physical process while other types of losses (e.g., financial) may involve a non-physical process. In either case, the first step is to understand what happened in the controlled process. While CAST can be (and has been) applied to losses involving other types of processes, such as business processes or even criminal and legal processes, the examples in this chapter focus on physical processes. The next chapter provides examples of applying CAST to social systems.

Explosions and fires are well-known hazards in chemical plants. There are usually a large number of protection systems, alarms, sensors, pressure relief valves, and so on. We start by examining the physical controls at the plant to determine why they did not control the explosion. At this point, a CAST analysis will not differ significantly from that done in most accident analysis except that in a CAST analysis, more than just physical failures are considered. For Shell Moerdijk, at the physical level, the CAST analysis would start by generating the following description of the physical controls:

| ID | 이벤트 | 제기된 질문 예제 |
|---|---|---|
| 10 | 지역사회 소방, 의료, 위기관리, 위기 커뮤니케이션이 시작되었다. | |

"실패"라는 단어는 사건에 대한 설명 어디에도 등장하지 않는다(물리적 컴포넌트의 실패가 발생하지 않는 한 CAST 분석 어느 곳에도 등장하지 않는다). "운영자들이… 했어야 한다"와 같은 사후 확신 편향 문장도 없다. 판단과 결론을 내리기엔 너무 이르다(이는 나중에라도 하지 말아야 한다). 또한 분석 초기에 식별된 질문들은 매우 일반적이다. 보다 많은 것을 알게 되면 이러한 질문들은 상세화 될 것이고 그에 대한 답변은 더 많은 질문을 만들어 낼 것이다. 결국 모든 질문에 답변하거나 답변할 수 없는지를 파악하는 것이 목표이다. 이 답변들을 통해서 사고가 발생한 이유와 컨트롤 및 보호 장치가 이벤트의 영향을 완화하지 못한 이유에 대해 깊게 이해하게 될 것이다.

여기서 제시된 이벤트 체인의 예는 "완전(complete)"와는 거리가 멀다(더 많은 이벤트들이 언제든 추가될 수 있기 때문에 그러할 수도 있음). 실제로 완전성은 CAST 분석 결과에 거의 영향을 미치지 않을 것이다. 이번이 아니더라도 답변해야 할 질문들은 나중에 만들어질 것이다. 명확하지 않다면 이벤트 체인이 간단한 시작점이 될 수는 있다. 다시 말하지만, CAST 분석을 할 때 반드시 이벤트 체인부터 시작해야 할 필요는 없다.

**제안:** 당신에게 익숙한 사고를 택하거나 어떤 일이 일어났는지 상세한 설명이 가능한 사고를 선택한다. 주요 이벤트를 적어라. 목록이 완성될 필요는 없다. 이것은 시작점일 뿐이다. 사건이 왜 일어났는지 파악하기 위해 이벤트와 관련된 질문들을 만들어라. 사고가 아주 간단한 경우가 아니면 질문은 거의 완성되지 않을 것이다. 당신이 만들어낸 질문은 당신의 생각의 출발점을 만든다. CAST 과정을 거치면서 더 많은 질문들이 만들어질(그리고 희망컨대 답변할 수 있을) 것이다.

## 컨트롤드 프로세스(Controlled Process)에서 일어나는 일의 이해

어떤 일이 "왜" 일어났는지를 파악하기 위해서는 먼저 "무엇"이 일어났는지 알아야 한다. 신체적 부상이나 손실은 반드시 물리적 프로세스를 수반하는 반면, 다른 유형의 손실(예: 재정)은 비 물리적인 프로세스를 수반할 수 있다. 두 경우 모두, 컨트롤드 프로세스에서 어떤 일이 일어났는지를 먼저 이해해야 한다. CAST는 비즈니스 프로세스나 형사 및 법률 프로세스와 같이 다른 유형의 프로세스에 관련된 손실에 적용될 수 있지만 이 장에서 제시하는 예는 물리적 프로세스에 중점을 둔다. 다음 장에서는 사회적 시스템에 CAST를 적용하는 사례를 제시한다.

화학 플랜트에서의 폭발과 화재는 잘 알려진 위험 요소이다. 플랜트에는 일반적으로 다수의 보호 시스템, 경보기, 센서, 압력 완화 밸브 등이 있다. 폭발을 통제하지 못한 이유를 파악하기 위해서는 플랜트의 물리적 컨트롤을 조사하는 것부터 시작한다. 이 시점에서의 CAST 분석은 분석 시 물리적인 실패 이상의 것을 고려한다는 점을 제외하고는 대부분의 사고 분석에서 수행하는 것과 크게 다르지 않다. 쉘 뫼르딕에 대한 물리적 수준의 CAST 분석은 다음과 같은 물리적 컨트롤에 대한 설명을 기술하면서 시작할 수 있다.

Requirements for hazard mitigation:

Provide physical protection against hazards (protection for employees and others within the vicinity)

1. Protect against runaway reactions
2. Protect against inadvertent release of toxic chemicals or explosion
3. Provide feedback about the state of the safety-critical equipment and conditions
4. Provide indicators (alarms) of the existence of hazardous conditions
5. Convert released chemicals into a non-hazardous or less hazardous form
6. Contain inadvertently released toxic chemicals
7. Provide physical protection against human or environmental exposure after release

Controls:

The physical safety equipment (controls) in a chemical plant are usually designed as a series of barriers to satisfy the above hazard mitigation requirements. The Shell Moerdijk plant had the standard types of safety equipment installed. Not all of it worked as expected, however.

Emergency and safety equipment related to this accident were:

1. An automatic protection system to release gas to flare tower
2. Pressure relief devices in case of overpressurization
3. Alarms
4. Temperature sensors in the reactor

Next, we determine what happened. What physical failures and interactions led to the hazard?

Failures: None of the physical controls failed except for the final collapse of the reactor and separation vessel after pressure reached a critical level.

Unsafe Interactions: Accidents often result from interactions among the system components. In this case, the following unsafe (and mostly unexpected) interactions occurred:

1. The process to distribute the ethylbenzene over the catalyst pellets (wet them) resulted in dry zones. There were two main reasons for these dry zones:
   - The nitrogen flow was too low. To wet the catalyst properly, an adequate amount of ethylbenzene and nitrogen in the correct ratio must pass through the distribution plate. Because the flow of nitrogen was too low, the distribution plate did not operate properly. Later, due to this problem, along with other unintended interactions, the pressure increased eventually to the point where it exceeded the flow of nitrogen to the reactor. The nitrogen flow came to a standstill, resulting in a negative pressure differential.
   - The flow of ethylbenzene was unstable and at times too low. In addition to a sufficiently high nitrogen flow, a constant and sufficient flow of ethylbenzene is required in order to properly wet the pellets. The two reactors of Unit 4800 have different diameters, which means that reactor 1 requires an ethylbenzene flow of approximately 88 tons per hour while reactor 2 needs approximately 22 tons per hour. A constant flow of this volume was achieved in reactor 1. A constant flow of the correct volume was also initially achieved for reactor 2. However, once ethylbenzene began being heated, the flow became unstable. In the last hour before the explosion, this flow was virtually zero on two occasions. As a result, the ethylbenzene was not

위험 완화를 위한 요구사항:

위험에 대한 물리적 보호(직원 및 인근 사람의 보호)를 제공한다.

1. 폭주 반응(runaway reaction)으로부터 보호
2. 의도하지 않은 독성 화학 물질 유출 또는 폭발로부터 보호
3. 안전 중요 장비 및 조건에 대한 피드백 제공
4. 위험 상태에 대한 지표(경보) 제공
5. 유출된 화학 물질을 위험하지 않거나 덜 위험한 형태로 전환
6. 부주의로 유출되는 독성 화학 물질을 억제
7. 유출 후 사람 또는 환경에 노출되지 않도록 물리적으로 보호

컨트롤:

화학 플랜트에서 물리적 안전 장비(컨트롤)는 일반적으로 위와 같은 위험 완화 요구사항을 충족시키기 위한 일련의 방어막으로 설계된 것이다. 셸 뫼르딕 플랜트는 표준형 안전 장비를 설치하였다. 하지만 모든 것이 예상대로 작동하지는 않았다.

이 사고와 관련된 비상 및 안전 장비는 다음과 같다.

1. 가스를 플레어 타워로 방출하는 자동 보호 시스템
2. 과압(overpressurization) 시 압력 완화 장치
3. 경보
4. 반응로의 온도 센서

다음으로, 우리는 무슨 일이 일어났는지 결정한다. 어떤 물리적인 실패와 상호작용이 위험을 초래했을까?

실패: 압력이 임계치에 도달한 후에는 반응로와 분리 용기의 최종 붕괴를 제외하고는 물리적 컨트롤 중 어느 것도 실패하지 않았다.

안전하지 않은 상호작용: 사고는 종종 시스템 구성요소 간의 상호작용에서 발생한다. 이 경우에서는 다음과 같은 안전하지 않은(그리고 대부분 예상치 못한) 상호작용이 발생했다.

1. 촉매제 펠릿에 에틸벤젠을 살포하는 공정(습윤)으로 건조한 구역이 발생했다. 이런 건조한 구역 발생에는 두 가지 주요한 이유가 있다.
   - 질소 유량이 부족했다. 촉매제를 충분히 적시려면 적당한 양의 에틸벤젠과 질소가 분배판을 통과해야 한다. 질소의 유량이 너무 적어 분배판이 제대로 기능하지 않았다. 나중에 이 문제는 결국 다른 의도하지 않은 상호작용과 함께 반응로에의 질소 유량을 초과하는 정도까지 압력을 증가시켰다. 질소 흐름이 정지되었고 이로 인해 음압(역주: 대기압보다 압력이 낮은 것) 차이가 발생하게 되었다.
   - 에틸벤젠의 흐름이 불안정했고 가끔은 너무 낮았다. 펠릿을 적절하게 적시기 위해서는 충분히 높은 질소 유량 외에도 일정하고 충분한 에틸벤젠 유량이 필요하다. Unit 4800의 두 반응로는 직경이 다른데, 반응로 1에는 시간당 약 88톤의 에틸벤젠 공급이 필요하고 반응로 2에는 시간당 약 22톤이 필요하다. 반응로 1에서 해당 용량에 맞게 일정한 에틸벤젠 공급이 이루어졌다. 또한, 초기에는 반응로 2에 대해서도 역시 정확한 양으로 일정하게 에틸벤젠 공급이 이루어졌다. 그러나 에틸벤젠이 가열되기 시작하면서 공급이 불안정해졌다. 폭발 전 마

evenly spread over the catalyst pellets, leading to the catalyst pellets not being adequately wetted and dry zones developing in reactor 2.

2. Energy released during the warming of the reactor led to unforeseen chemical reactions between the warming up liquid (ethylbenzene) and the catalyst pellets in the dry zones. As heating took place, the ethylbenzene began to react with one of the catalyst elements (barium chromate), generating heat. The ethylbenzene dissipated this heat in the areas that were sufficiently wetted. In the dry zones, however, this heat did not dissipate due to the lack of ethylbenzene. The result was that in the dry zones, the catalyst pellets heated up considerably, and there was localized development of very hot areas or "hotspots." The hotspots were not automatically detected due to the limited number of temperature sensors in the reactors.
3. Due to the rising temperature, the reaction in the hotspots kept accelerating, thereby producing even more heat. The localized temperature was now very high, which resulted in a chemical reaction between the ethylbenzene and another catalyst element (copper oxide). This reaction caused gases to be released. These follow-on reactions reinforced each other and could no longer be stopped: a runaway had developed. The rapidly rising temperature led to localized ethylbenzene evaporation.
4. Gas formation increased the pressure in the reactor. At the same time, the maximum liquid level in the second separation vessel was exceeded, causing the automatic protection system (used to release excess pressure) to shut down automatically in order to prevent liquids from entering the exhaust gas system (flare). As a result, the gases in the system could no longer be discharged. This automatic protection device to prevent liquids from entering the flare operated as designed, but had the unintended consequences of preventing the venting of the gas.
5. The buildup of gas caused the pressure to increase. Eventually, the pressure reached the point where the automatic pressure relief devices in place could not adequately release it. The pressure relief devices on the separation vessels were not designed for such rapid pressure increases, and eventually the collapse pressure of the reactors was reached. Reactor 2 collapsed and exploded, followed 20 seconds later by the explosion of the first separation vessel.
6. The contents of reactor and the separation vessel spread beyond the boundary of Unit 4800. A pressure wave and hot, burning catalyst pellets hit workers in the area causing injuries.
7. There are three remote-controlled containment valves. The explosions made these valves ineffective. The alternative was to use other limiting valves, but these valves cannot be remotely operated (they must be operated manually). Due to the intensity of the fire that had broken out and the risk of explosion, it was not possible for these to be operated immediately. An initial attempt was made around 02:30.

The above section shows why one does not need to start by listing the proximal events in isolation from the CAST analysis. The important events (failures and unsafe interactions) will be identified here as well as questions arising from these events.

After addressing what happened, we need to look at why it happened. Most of the reasons will be found in the later analyses, but physical design deficiencies and contextual factors are included here.

지막 한 시간 동안에는 두 차례 공급량이 거의 0이었다. 그 결과, 에틸벤젠이 촉매제 펠릿 위에 고르게 퍼지지 않아 촉매제 펠릿이 적절하게 젖지 않았고 반응로 2에 건조한 구역이 발생하였다.

2. 반응로를 데우면서 방출된 에너지는 건조 구역의 데워진 액체(에틸벤젠)와 촉매제 펠릿 사이에 예상치 못한 화학 반응을 야기했다. 가열이 진행되면서 에틸벤젠은 촉매제 성분 중 하나(바륨 크로메이트)와 반응하기 시작하여 열을 발생시켰다. 에틸벤젠이 충분히 젖은 영역에서는 이 열이 소멸되었다. 그러나 건조 구역에서는 에틸벤젠 부족으로 인해 열이 소멸되지 않았다. 그 결과 건조 구역에서 촉매제 펠릿이 상당히 가열되었고, 매우 뜨거운 지역 또는 "핫스팟"이 국지적으로 생성되었다. 반응로의 온도 센서 개수가 한정되어 있어 핫스팟이 자동으로 검출되지 않았다.

3. 온도 상승으로 인해 핫스팟의 반응이 계속 가속화되어 더 많은 열이 발생했다. 이제 국소적으로 온도가 매우 높아졌고, 그 결과 에틸벤젠과 다른 촉매제 요소(산화구리) 사이에 화학적 반응이 일어났다. 이 반응으로 가스가 방출되었다. 이 후속 반응은 두 성분 간의 반응을 증가시켰고 더 이상 컨트롤 할 수 없게 되었다: 즉, 폭주가 시작되었다. 급속한 온도 상승은 국소적인 에틸벤젠 증발을 야기했다.

4. 가스 발생은 반응로의 압력을 증가시켰다. 동시에 두 번째 분리 용기의 최대 액체 레벨이 초과되었고, 액체가 배기가스 시스템(플레어)으로 들어가는 것을 방지하기 위해 자동 보호 시스템(과다 압력을 방출하는 데 사용됨)이 자동으로 셧다운 되었다. 그 결과, 시스템내의 가스가 더 이상 배출될 수 없었다. 액체가 플레어로 유입되는 것을 방지하기 위한 이 자동 보호 장치는 설계된 대로 작동했지만 의도하지 않게 가스 배출을 막는 결과를 야기하였다.

5. 가스의 축적은 압력을 더욱 증가시켰다. 결국 자동 압력 완화 장치가 가스를 적절히 방출할 수 없는 지점까지 압력이 도달했다. 분리 용기의 압력 완화 장치 설계 시 이러한 빠른 압력 증가가 고려되지 않았으며 결국 반응로 붕괴 압력에 도달했다. 반응로 2는 붕괴되고 폭발했으며, 20초 후 첫 번째 분리 용기의 폭발로 이어졌다.

6. 반응로와 분리 용기의 내용물은 Unit 4800의 경계를 넘어 확산되었다. 압력파와 불타는 촉매제 펠릿이 그 지역의 작업자들을 가격하여 부상을 입혔다.

7. 원격 제어용 격납 밸브가 세 개 있었다. 하지만 폭발로 인해 이 밸브들의 기능이 상실되었다. 대안은 다른 제한 밸브를 사용하는 것이었지만, 그 밸브는 원격으로 작동할 수 없었다(수동으로 작동해야 한다). 화재의 강도와 폭발 위험 때문에 이들을 즉시 작동시키는 것이 불가능했고 2시 30분경에 처음 작동을 시도할 수 있었다.

위 섹션은 CAST 분석과는 별도로, 우리가 근접 이벤트를 나열하여 시작할 필요가 없는 이유를 보여준다. 여기서는 이벤트와 관련하여 발생하는 질의사항 뿐만 아니라 중요한 이벤트(실패 및 안전하지 않은 상호작용)도 식별하게 될 것이다.

무슨 일이 있었는지를 언급한 후에, 왜 그런 일이 일어났는지 살펴보아야 한다. 대부분의 원인은 이후 분석에서 찾을 수 있겠지만 물리적 설계 결함과 컨텍스트적 요인은 이 과정에서 파악될 수 있다.

Missing or inadequate plant physical controls that might have prevented the accident:

1. There was an inadequate number of temperature sensors in the reactor to detect hot spots.
2. The plant was not fitted with pressure relief valves that would have prevented a runaway. Those that were installed were not designed for the rapid pressure increases that occurred.

Contextual Factors:

1. The plant was out of operation for a short, scheduled maintenance to replace the catalyst-causing granules.
2. Unexpected reactions occurred due to vulnerabilities related to the design, including the:
   - Potential for insufficient wetting (hot spots) due to design flaws.
   - Use of ethylbenzene and a design assumption that this substance is inert in the presence of the catalyst pellets.

Summary of the Role of the Physical Components in the Accident: None of the physical controls failed. The final physical collapse of the reactor and separation vessel occurred after pressure reached a critical level, which resulted from unexpected and unhandled chemical and physical interactions. Many of these unsafe interactions were a result of design flaws in the reactor or in the safety-related controls.

There are some things to be noted in this description. The description is restricted to the physical system. Operators, process control systems, etc. are not—and should not be—mentioned. The role they played will be considered later.

Also, remember that the accident model (STAMP) underlying CAST says that accidents result from lack of control, which may include control of failures. In this part of the analysis, an understanding is gained about why the physical controls were unsuccessful. Controls are used to enforce constraints on the behavior of the system components and the system as a whole and the identification of the inadequate controls will assist in refining the high-level system hazards and the safety constraints needed to prevent the hazards.

The original hazards and constraints were very general and apply to almost any chemical plant process. In fact, these could be identified for an industry as a whole and used for any accidents. Identifying the specific failures and unsafe interactions that occurred in the physical process will allow the general system hazard and safety constraints to be refined for this particular loss and therefore provide increased direction for the causal analysis.

As an example, in the Shell Moerdijk case, the general constraint to keep chemicals under positive control can now be refined to identify the specific constraints that were violated and thus the specific goals for this accident analysis:

1. Chemicals must be under positive control at all times, i.e., runaway reactions must be prevented (see the general Safety Constraint 1 under System Hazard 2 on page 37).
   a. Distribution of ethylbenzene over the catalyst pellets must not result in dry spots during a reactor restart.
   b. Protection and warning systems must be created to react to the heat and pressure generated by unintended reactions related to dry spots if they nonetheless occur.

사고를 예방할 수 있는 플랜트의 물리적 컨트롤이 누락되거나 부적절한 경우:

1. 반응로 내에 핫스팟을 감지하기 위한 온도 센서의 개수가 부족했다.
2. 폭주를 막을 수도 있는 압력 완화 밸브가 갖추어져 있지 않았다. 설치되어 있는 밸브는 급격한 압력 증가를 대비하도록 설계되지 않았다.

컨텍스트적 요인:

1. 촉매 유발 과립제 교체 목적으로 짧게 예정된 유지보수 수행을 위해 플랜트 가동이 중지된 상태였다.
2. 다음과 같은 설계 관련 취약점 때문에 예상치 못한 결과가 발생하였다.
   - 설계 결함으로 인한 불충분한 습윤(핫스팟) 가능성
   - 에틸벤젠의 사용한 것, 그리고 촉매제 펠렛의 존재 하에서는 에틸벤젠이 불활성이라는 설계 가정

사고 시 물리적 구성요소의 역할 요약: 물리적 컨트롤 중 어느 것도 실패하지 않았다. 반응로와 분리용기의 최종 물리적 붕괴는 압력이 임계 수준에 도달한 후에 발생했으며, 이는 예기치 않은 화학적 및 물리적 상호작용으로 인한 것이다. 이러한 안전하지 않은 상호작용 중 많은 부분은 반응로 또는 안전 관련 컨트롤의 설계 결함에 따른 결과였다.

이 설명에는 몇 가지 유의할 점이 있다. 설명이 물리적 시스템에 국한되어 있다는 점이다. 운영자, 프로세스 컨트롤 시스템 등은 언급되지 않았으며 언급되어서도 안 된다. 이들이 담당하는 역할은 나중에 고려될 것이다.

또한 CAST의 기반이 되는 사고 모델(STAMP)에서, 사고는 컨트롤의 부족에서 기인한 것으로 보며 여기서 컨트롤의 부족에는 컨트롤의 실패가 포함된다. 분석 과정에서는 물리적 컨트롤이 실패한 이유를 파악한다. 컨트롤은 시스템 구성요소와 시스템의 전체 동작에 대해 제약사항을 강제하기 위해 사용되며, 따라서 부적절한 컨트롤의 식별은 위험을 방지하기 위해 필요한 상위 수준의 시스템 위험 및 안전 제약사항을 개선하는 데 도움이 된다.

근본적인 위험과 제약사항은 매우 일반적이고 거의 대부분의 화학 플랜트 공정에 적용된다. 사실, 이는 산업 전반에 걸쳐 식별될 수 있고 어떤 사고에도 적용될 수 있다. 물리적 공정에서 발생한 특정 실패와 안전하지 않은 상호작용을 식별하는 것은 이 특정 손실에 대해 일반적인 시스템 위험 및 안전 제약사항을 개선할 수 있고 원인 분석을 위한 방향 설정에도 도움이 될 것이다.

예를 들어 쉘 메르딕의 경우 화학 물질을 정상적 상태 내에서 유지하기 위한 일반적인 제약사항은, 위반된 특정 제약사항을 식별하기 위해 상세화되거나 이 사고 분석의 구체적 목표를 식별하기 위해 상세화 될 수 있다.

1. 화학물질은 항상 정상적인 상태 내에서 유지되어야 한다. 즉, 폭주 반응을 방지해야 한다. (37페이지의 시스템 위험 2에 따른 일반 안전 제약사항 1 참조)
   a. 반응로 재시작 과정에서 촉매제 펠릿에 에틸벤젠을 살포하는 것이 건조한 구역을 발생하도록 해서는 안 된다.
   b. 그럼에도 불구하고 건조한 구역이 발생한다면, 건조한 구역과 관련된 의도하지 않은 반응에 의해 발생하는 열과 압력에 대응하도록 보호 및 경고 시스템을 만들어야 한다.

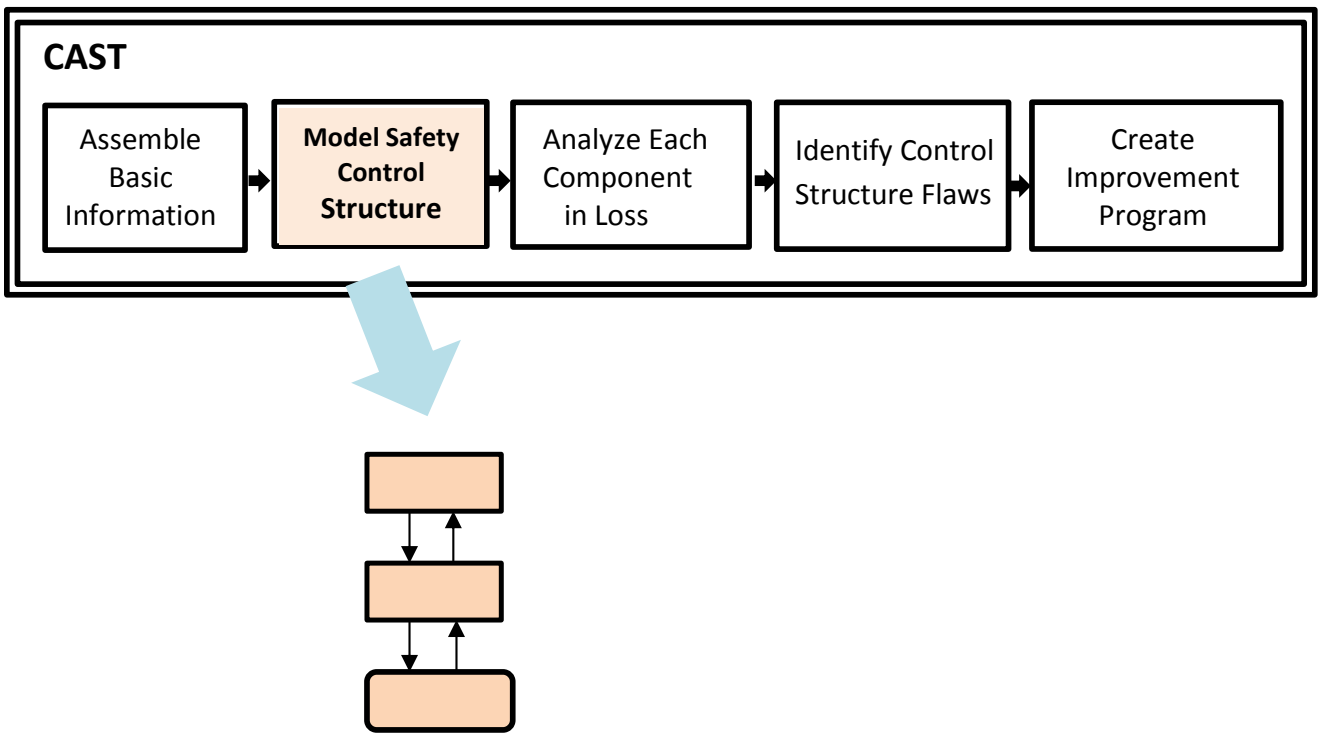
Constraints are theoretically enforced either through eliminating the related hazardous states from the physical system design, providing controls in the physical design to prevent or minimize the hazard, or providing operational controls. Usually, all are used as engineering design can almost never be perfect. So, the goal of the analysis now is to identify why the design flaws were introduced, i.e., why the attempts to enforce the constraints through physical design were ineffective and why the operational controls also were not successful.

To achieve this analysis goal, we start by looking at the safety control structure to identify its limitations in preventing the accident. Normally, both system development and system operations need to be included. Too often, accident analysis only focuses on operations and not system development and, therefore, only operational limitations are considered. Deficiencies in the way the system was developed are not always identified or fully understood.

이론적으로 제약사항은 위험을 방지하거나 최소화시키기 위해 물리적 시스템 설계에서 관련 위험 상태를 제거하거나, 물리적 설계에 컨트롤을 추가하거나, 운영상 컨트롤을 추가함으로써 강제된다. 일반적으로 엔지니어링 설계에 사용되는 어떤 것도 절대 완벽할 수는 없다. 따라서 분석의 목표는 설계상의 결함이 존재하게 된 이유, 즉 물리적 설계를 통해 제약사항을 강제하는 시도가 왜 효과적이지 않았는지, 운영상 컨트롤 역시 왜 성공하지 못했는지를 파악하는 것이다.

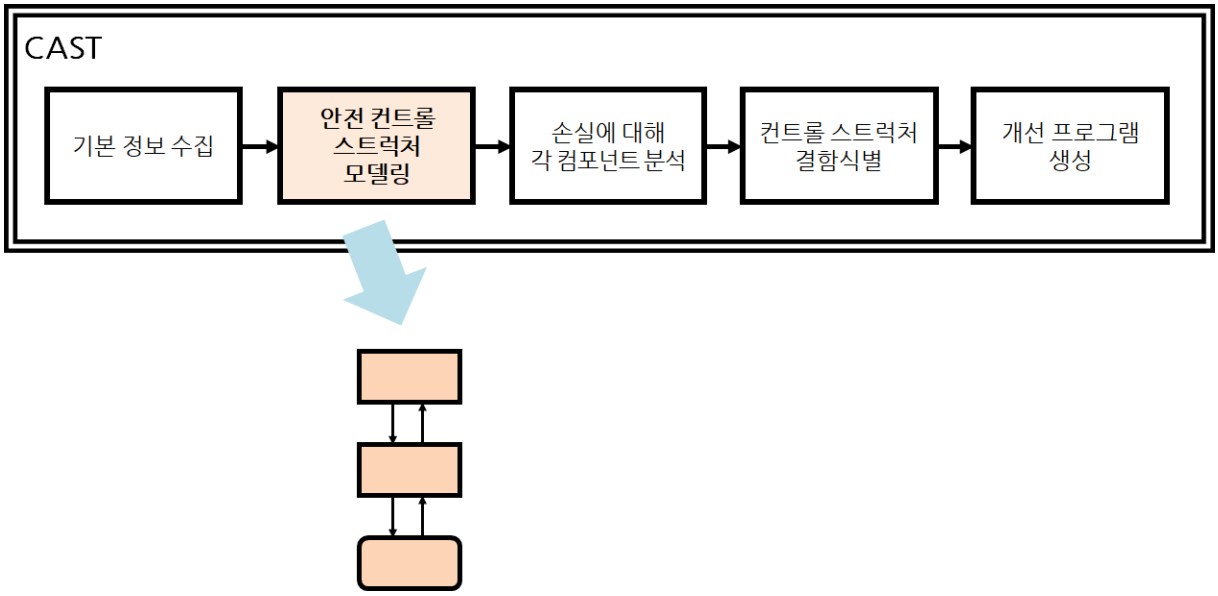
우리는 이러한 분석 목표를 달성하기 위하여 안전 컨트롤 스트럭처를 살펴보고 안전 컨트롤 스트럭처가 사고 예방에 미치는 한계를 파악한다. 일반적으로 시스템 개발과 시스템 운영 측면을 모두 고려해야 한다. 사고 분석은 종종 시스템 개발 측면은 배제하고 운영 측면에만 초점을 맞추게 되어 운영상 한계만 고려하는 경우가 너무 많다. 시스템 개발 과정에서의 결함을 항상 식별하거나 완전하게 이해할 수 있는 것은 아니다.

## Modeling the Safety Control Structure[15]




[15] A more common name for the safety control structure is the Safety Management System (SMS), although some standards for safety management systems are incomplete with respect to the safety control structure. The safety control structure includes functions and components not always in an SMS.

## 안전 컨트롤 스트럭처 모델링[15]




15 안전 컨트롤 스트럭처 측면에서 안전 관리 시스템(SMS, Safety Management System)의 일부 표준이 완전하지 않기는 하나, 안전 컨트롤 스트럭처의 더 일반적인 명칭은 안전 관리 시스템(SMS)이다. 안전 컨트롤 스트럭처에는 안전 관리 시스템에 포함되지 않는 기능 및 컴포넌트도 포함될 수 있다.

2. *Model the existing safety control structure for this type of hazard.*

The model of causality underlying CAST treats safety as a *control* problem, not a *failure* problem. The cause is always that the control structure and controls constructed to prevent the hazard were not effective in preventing the hazard. The goal is to determine why and how they might be improved.

Because CAST focuses on the controls and controllers and their role in the accident, modeling the control structure is necessary to start the analysis. There is no single or best way to accomplish this, assuming that a safety control structure for that system and the hazards identified in the previous step does not already exist. But there are some hints or heuristics that may help. The two most helpful are to (1) start with a very high-level, abstract control structure and then refine it later and (2) start by identifying the controls that exist for the hazard or hazards in general. These two activities may be done separately or the activities may be intertwined.

Usually, similar accidents have occurred previously, and controls have been created to prevent them. The major goal of the analysis in that case, as stated above, is to determine why they were not effective and how to improve them. Some of the controls will be common safety practices, while others may be special controls designed for unique situations. All the controls need not be identified at first. The questions generated as the analysis proceeds will identify more constraints and controls. The only mistake is to start too narrowly as this might cause you to miss important controls and controllers or system hazards. Important clues in identifying controls can usually be obtained from the original hazard analysis on the plant, assuming a hazard analysis was done that goes beyond simply identifying probabilities of component failures in order to assess the risk of the completed design.

If STPA was used for designing the system, there will be an explicit listing of the scenarios leading to an accident that were identified and the controls created during system development. If an STPA analysis for the system already exists, then it will provide a lot of information about what might have gone wrong. Theoretically, the STPA analysis should contain the scenario that occurred. If not, then there was a disconnect between the analysis during development and the operation of the system. One possibility is that the original STPA did not completely specify all the potential scenarios. Another is that the scenario that occurred was identified, but an effective control was not implemented. And, of course, the system and its environment may have changed over time after the system went into operation, negating the effectiveness of the designed controls and introducing new causal scenarios that were not analyzed originally.

If a control structure for the system does not already exist, most people find it helpful to start with a very abstract, high-level control structure that involves the general controls for this type of event. Figure 13 shows a preliminary, very high-level safety control structure for Shell Moerdijk. There are two physical processes being controlled: chemical production and public health.

The Shell Moerdijk plant has direct responsibility for control of the safety of the chemical process itself while state and local emergency management have the responsibility for preserving public health. The global Shell enterprise exerts control over the subsidiaries and Shell plants around the world. At this early point in the analysis, the type of control and responsibilities will be mostly unknown. These will need to be elaborated during the investigation. With respect to government oversight, there are local and Dutch oversight agencies and overarching EU controls. It is usually helpful to document the responsibilities (as understood so far) for each of these components with respect to the hazards involved. Again, the model will change as more information is accumulated during the investigation.

*2. 이러한 유형의 위험에 대한 기존의 안전 컨트롤 스트럭처를 모델링한다.*

CAST의 기초가 되는 인과관계 모델에서는 안전을 *실패* 문제가 아니라 *컨트롤* 문제로 취급한다. 위험을 방지하기 위해 구축된 컨트롤 스트럭처와 컨트롤이 위험을 방지하는 데 항상 효과적인 것은 아니기 때문이다. 따라서 이러한 문제를 개선할 방법과 이유를 결정하는 것이 목표이다.

CAST는 컨트롤, 컨트롤러 및 사고에서의 이들의 역할에 초점을 맞추고 있기 때문에 분석을 시작하기 위해서는 컨트롤 스트럭처 모델링이 필요하다. 시스템에 대한 안전 컨트롤 스트럭처와 이전 단계에서 식별된 위험에 대한 정보가 없다고 가정하면, 모델링을 하는 방법은 한 가지가 아니며 최선의 방법이 있는 것도 아니다. 하지만 도움이 될 만한 몇 가지 힌트나 휴리스틱(heuristic) 방법은 있다. 가장 유용한 두 가지 방법은 (1) 매우 상위 수준의 추상적 컨트롤 스트럭처로 시작하여 나중에 상세화하는 것 (2) 위험 또는 위험이 존재하는 컨트롤을 전반적으로 식별하는 것이다. 이 두 활동은 별도로 수행될 수도 있고 서로 밀접하게 연관되어 있을 수도 있다.

일반적으로 과거에 발생한 사고와 유사한 사고를 방지하기 위해 컨트롤이 만들어졌다. 이 때 분석의 주요 목표는 위에서 말한 바와 같이 그것들이 왜 효과적이지 않은지 그리고 어떻게 개선할지를 결정하는 것이다. 어떤 컨트롤은 일반적인 상황에 대한 것이며 어떤 컨트롤은 특수한 상황을 위해 설계된 특수 컨트롤일 수 있다. 처음부터 모든 컨트롤을 식별할 필요는 없다. 분석이 진행됨에 따라 발생하는 질문들을 통해 더 많은 제약사항 및 컨트롤을 식별할 것이다. 여기서 발생할 수 있는 유일한 실수는 너무 제한적으로 시작하여 중요한 컨트롤 및 컨트롤러 또는 시스템 위험을 놓칠 수도 있다는 것이다. 완성된 설계의 리스크 평가를 위해 위험 분석이 단순히 컴포넌트 실패 확률을 식별하는 것을 넘어 수행되었다면, 컨트롤 식별에서의 중요한 단서는 플랜트의 기존 위험 분석 결과에서 얻을 수 있다.

시스템 설계에 STPA가 사용되었다면 파악된 사고로 이어지는 시나리오 목록과 시스템 개발 과정에서 만들어진 컨트롤 목록이 분명히 있을 것이다. 만약 시스템에 대한 STPA 분석 결과가 이미 존재한다면 그 결과에서 무엇이 잘못되었는지에 대한 많은 정보를 알 수 있을 것이다. 이론적으로 STPA 분석은 실제 발생했던 시나리오를 포함해야 한다. 그렇지 않으면 개발 과정에서의 분석과 실제 시스템 운영 사이의 불일치가 발생할 것이다. 불일치에 대한 원인으로 원래의 STPA가 모든 잠재적 시나리오를 완전히 명시하지 않았을 수도 있다. 또 다른 원인으로 발생한 시나리오는 확인되었지만 효과적인 컨트롤이 구현되지 않았을 수도 있다. 물론 시스템 작동 후 시간이 지남에 따라 시스템 및 시스템 운영 환경이 바뀌었을 수 있으며 설계된 컨트롤의 효과를 부정하고 기존에 분석되지 않았던 새로운 원인 시나리오를 도입했을 수 있다.

기존에 만들어진 시스템의 컨트롤 스트럭처가 없다면 이러한 유형의 이벤트에 대한 일반적인 컨트롤을 포함하는 매우 추상적이고 상위 수준의 컨트롤 스트럭처로 시작하는 것이 도움이 된다고 많은 사람들이 말했다. 그림 13은 쉘 뫼르딕의 매우 상위 수준의 예비 안전 컨트롤 스트럭처를 보여준다. 화학물질 생산과 공중 보건이라는 두 가지 물리적 프로세스가 컨트롤되고 있다.

쉘 뫼르딕 플랜트는 화학 공정 자체의 안전을 컨트롤하는 직접적인 책임이 있으며 주(state) 및 지방 비상 관리 조직은 공중 보건을 지킬 책임이 있다. 세계적인 쉘 기업은 전 세계 자회사와 쉘 플랜트를 컨트롤한다. 분석 초기 시점에는 컨트롤과 책임의 유형이 거의 알려지지 않았을 것이다. 이것은 조사 과정에서 상세화해야 할 것이다. 정부 감독과 관련하여 지방, 네덜란드의 감독 기관, 그리고 가장 중요한 EU의 컨트롤이 있다. 일반적으로 연관된 위험과 관련하여 이들 컴포넌트 각각에 대한 책임을 문서화하는 것이(지금까지 이해한 바와 같이) 도움이 된다. 다시 말하지만 조사 과정에서 많은 정보가 축적될수록 모델은 변화될 것이다.

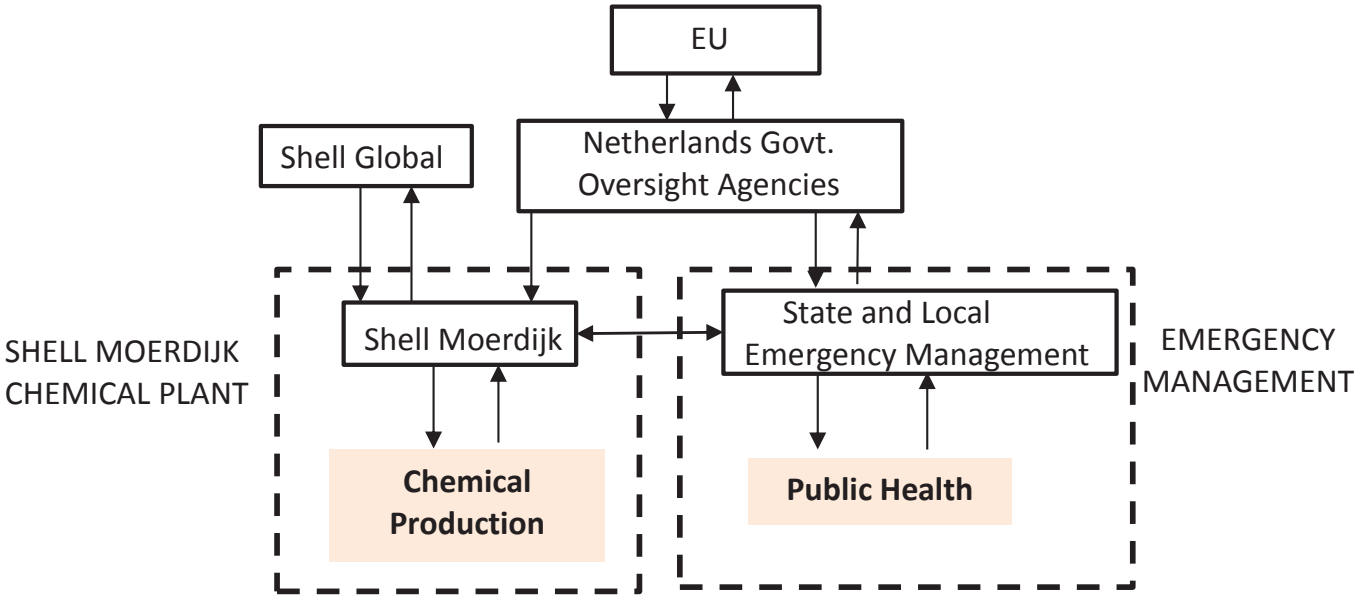



**Figure 13**: Very high-level safety control structure model for Shell Moerdijk.

In the process of creating the model, it may be helpful to first identify what types of controls exist both in general and in this particular system, for preventing the hazard. Once you have started the list of controls (you will probably add to it later), consider where responsibility for them exists in the physical design, human controllers, automation, or organization and social structure. For example, there will probably be physical controls (such as interlocks and relief valves), electronic controls (such as ground proximity warning systems on aircraft), electronic process control systems that monitor and adjust process parameters, human operators, equipment maintainers, management oversight, regulatory controls, and so on.

After the controls have been identified, modeling the hierarchy—to show what controls what—should be the only remaining challenge. Don't be surprised if you have some difficulty with this at first and end up making several changes. If you start with a high-level safety control structure, you should be able to place the controls in the structure as you discover them. As you proceed, more details can be added.

The control structure will probably also change as the investigation and understanding of the system develop. It may be helpful to make any changes first at the highest level that they are visible. Changes in the high-level control structure can lead to multiple changes at a lower level of abstraction. First making changes at a high-level will help to identify where extensive revisions in the control structure may be needed. For example, let's say you find late in the analysis process that maintenance was involved. Rather than try to add maintenance to the very detailed control structure developed by that time and include all the interactions it might have with other system components, it may be easier to go back to a high-level structure and add maintenance as a controller of the equipment and understand its relationship with other controllers. Once the overall role and place of maintenance in the system is modeled, more detailed control structures can be modified to include their relationships with maintenance controls.

Usually, the controls to prevent an accident are distributed around the control structure to the groups or system components best able to enforce the constraints and controls. Higher level components will have more general responsibilities, including the responsibility to oversee the operation of controls by the components below. For example, human operators may be responsible for adjusting physical parameters in the controlled process. Operations management may be responsible

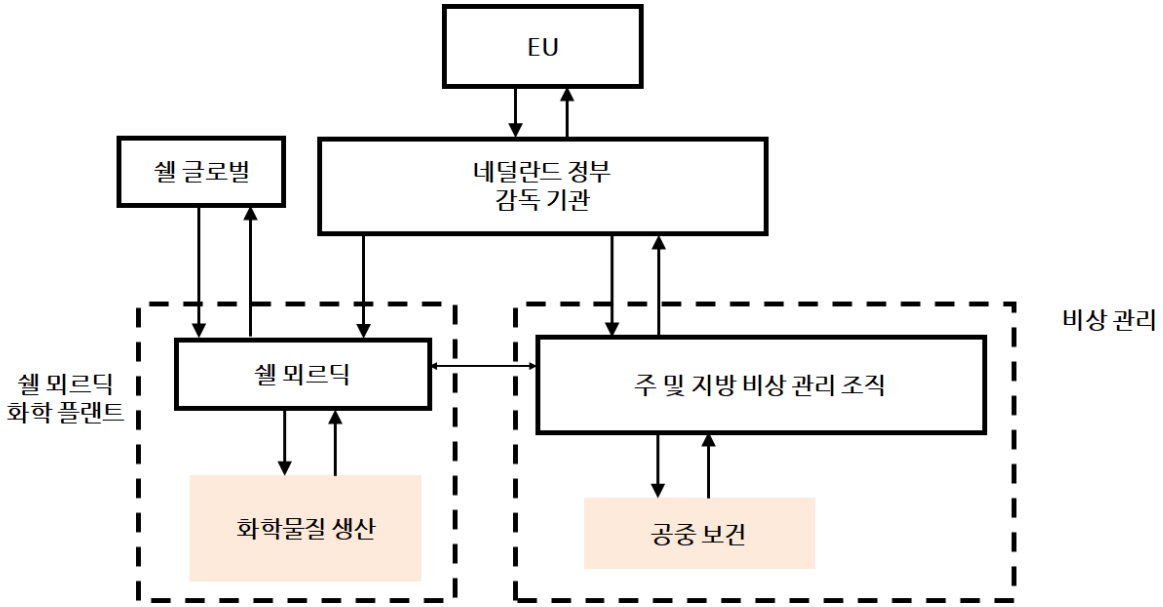



그림 13: 쉘 뫼르딕 플랜트에 대한 매우 상위 수준의 안전 컨트롤 스트럭처 모델

모델을 만드는 과정에서 일반적으로 어떤 유형의 컨트롤이 존재하는지, 그리고 특정 시스템에서 위험을 방지하기 위해 어떤 종류의 컨트롤이 존재하는지 우선적으로 확인하는 것이 도움이 될 수 있다. 일단 컨트롤 목록을 작성하기 시작하면(아마도 이후에 목록이 보완될 될 것임) 물리적 설계, 휴먼 컨트롤러, 자동화 또는 조직 및 사회 구조에서 그 컨트롤에 대한 책임이 어디에 존재하는지 고려한다. 예를 들어 물리적 컨트롤(인터락 및 릴리프 밸브와 같은), 전자적 컨트롤(항공기의 지상 접근 경고 시스템과 같은), 프로세스 파라미터를 모니터링 및 조정하는 전자 프로세스 컨트롤 시스템, 운영자, 장비 유지관리자, 관리 감독, 규제 제어 등이 있을 것이다.

컨트롤이 식별된 후에는 무엇이 무엇을 컨트롤하는지 보여주기 위한 계층 구조를 모델링하는 것이 남아있는 유일한 과제일 것이다. 처음에 약간의 어려움을 겪고 여러 차례 변경을 하게 되더라도 놀라지 않아도 된다. 상위 수준의 안전 컨트롤 스트럭처로 시작했다면 컨트롤에 대해 알게 됨에 따라 컨트롤을 스트럭처에 배치할 수 있을 것이다. 점차 진행됨에 따라 더 많은 세부사항이 추가될 수 있다.

시스템 개발에 대한 조사 및 이해도에 따라 컨트롤 스트럭처도 변경될 것이다. 가장 상위 수준에서 눈에 띄는 내용을 우선적으로 변경하는 것이 좋을 것이다. 상위 수준 컨트롤 스트럭처를 변경하면 하위 수준의 추상화에서 여러 가지 변경이 발생할 수 있다. 상위 수준에서 변경을 시작하는 것은 컨트롤 스트럭처에서 광범위한 수정이 필요할 수 있는 위치를 식별하는 데 도움이 될 것이다. 예를 들어 분석 프로세스 중 유지보수가 관련되어 있다는 사실을 늦게 발견했다고 가정해보자. 그 시점까지 개발된 매우 상세한 컨트롤 스트럭처에 유지보수를 추가하고 다른 시스템 컴포넌트와의 모든 상호작용을 포함하는 것 보다는 상위 수준의 컨트롤 스트럭처로 돌아가서 장비 컨트롤러로 유지보수를 추가하고 다른 컨트롤러와의 관계를 이해하는 것이 더 쉬울 수 있다. 시스템에서 유지보수의 전반적인 역할과 위치가 모델링되면 컨트롤 스트럭처가 유지보수 컨트롤과의 관계를 포함하도록 더 상세하게 수정될 수 있다.

일반적으로 사고를 방지하기 위한 컨트롤은 제약사항과 컨트롤을 가장 잘 강제할 수 있는 컨트롤 스트럭처 주위의 그룹 또는 시스템 컴포넌트에 분산되어 있다. 상위 수준의 컴포넌트는 하위 컴포넌트에 의한 컨트롤 작동을 감독하는 책임을 포함하여 보다 일반적인 책임을 가지게 된다. 예를 들어 운영자는 컨트롤드 프로세스에서 물리적 파라미터를 조정할 책임이 있을 수 있다. 운영 관리자는 작업자

for providing the training needed by the operators to perform their responsibility reliably and for hiring workers with appropriate backgrounds. Operations management probably will also be responsible for monitoring performance during operations to ensure that operators are performing adequately. Higher levels of management may ensure that training is taking place (but usually not the responsibility for specifying the details of that training) and that operations management is performing acceptably. The highest levels of corporate management and external regulatory oversight will be at yet a higher level of abstraction and detail. Together, the entire safety control structure should ensure that hazards are eliminated or controlled and safety constraints on the system behavior are enforced.

Once again, everything need not be identified at first in the causal analysis. Generating the questions and answering them as the analysis proceeds, will identify more controls and even constraints. Once several CAST analyses exist for a certain type of loss, the controls probably will have been identified in previous analyses. This step then becomes straightforward and simply involves finding unique controls for the particular loss involved. Why the controls were effective is part of the next step in the analysis. In this step, they are only listed.

Here is a demonstration of the refinement process for the Shell Moerdijk control structure, starting with the very high-level control structure in Figure 13. You need not generate a complete and final control structure at this point. Changes will likely be made and even structures added as the investigation proceeds. The goal is just to identify the controllers and their responsibilities to start the detailed CAST analysis.

Explosions and fires are well-known hazards in chemical plants, and controls are always included to prevent them. Controls will usually involve protection systems, alarms, sensors, pressure relief valves, and so on. Beyond the physical protection systems, there will usually be operators, process control systems, and safety management. Above them are various levels of management for these system components and for plant operations in general. A safety group usually exists that oversees both development and operations from a safety standpoint. This group may be responsible for various types of hazard analysis and risk assessment activities. Figure 14 includes the catalyst supplier (although it could be added later if the catalyst's role is not yet apparent) because the events point to a runaway reaction while the catalyst was being reheated. If it is not needed to explain the accident, then it can be removed later or it could be added later if omitted at this point. While the control structure can guide the analysis and make it easier to identify missing causal analysis, its major use is in the final report to help provide a coherent explanation of the accident, why it occurred, and what needs to be changed.

Responsibility for design activities rests somewhere; in the case of Shell Moerdijk, local design groups develop plant designs (not shown in Figure 14 but assumed to be under the control of and part of plant management) which are overseen or reviewed by Shell Projects and Technology at the Global level. There is also always some type of safety management at the corporate or global level. Finally, executive management (at least at the Board of Directors level) almost always has some type of corporate responsibility and oversight of safety at the enterprise management level. Here is what the control structure might look like at this point:

가 책임을 안정적으로 수행하기 위해 필요한 훈련을 제공하고 적절한 백그라운드를 가진 작업자를 고용하는 책임을 가질 수 있다. 운영 관리자는 작업자가 적절하게 수행하고 있는지 확인하기 위해 운영 중 성과를 모니터링 할 책임이 있다. 관리자 수준이 높을수록 훈련이 수행되고 있고(보통 해당 훈련의 세부내용을 명시할 책임은 없음) 운영 관리가 허용 가능한 수준으로 수행되고 있음을 보장할 수 있다. 기업 최고 경영진 및 외부 규제기관의 감독은 그보다 더 높은 수준의 추상화 및 세부 사항일 것이다. 동시에, 전체 안전 컨트롤 스트럭처는 위험을 제거하거나 통제하고 시스템 동작에 안전 제약사항이 강제되도록 보장해야 한다.

다시 말해 원인 분석 과정에서 처음부터 모든 것을 식별할 필요는 없다. 분석이 진행됨에 따라 질문을 하고 답변하면서 더 많은 컨트롤과 제약사항을 식별할 수 있다. 특정 유형의 손실에 대해 여러 CAST 분석이 여러 번 이루어졌다면 아마 이전 분석에서 컨트롤이 식별되었을 것이다. 만약 그렇다면 이 단계는 간단해지며, 단순히 관련된 특정 손실에 대한 특수한 컨트롤을 찾기만 하면 된다. 컨트롤이 효과적인지 여부에 대한 분석은 다음 단계에 나온다. 이 단계에서는 목록을 나열할 뿐이다.

아래 그림은 그림 13에 있는 매우 상위 수준의 컨트롤 스트럭처에서 시작한 쉘 뫼르딕 컨트롤 스트럭처의 상세화 프로세스를 보여준다. 이 시점에서 완전하고 최종적인 컨트롤 스트럭처를 생성할 필요는 없다. 조사가 진행됨에 따라 변경이 이루어지고 구조가 추가될 수 있다. 상세한 CAST 분석을 시작하기 위해 컨트롤러 및 컨트롤러의 책임을 확인하는 것이 목표이다.

폭발 및 화재는 화학 플랜트에서 잘 알려진 위험이며 이를 방지하기 위한 컨트롤이 항상 마련되어 있다. 컨트롤에는 일반적으로 보호 시스템, 경보, 센서, 압력 완화 밸브 등이 포함된다. 물리적 보호 시스템 외에도 일반적으로 운영자, 프로세스 컨트롤 시스템 및 안전 관리가 있다. 그 상위에는 일반적으로 이러한 시스템 컴포넌트 및 플랜트 운영에 대한 다양한 수준의 관리가 있다. 안전의 관점에서 보면 일반적으로 개발 및 운영을 모두 감독하는 안전 그룹이 존재하며, 이 그룹은 다양한 유형의 위험 분석 및 리스크 평가 활동을 담당할 수 있다. 그림 14에는 촉매제 공급 업체가 포함되어 있는데(촉매제의 역할이 아직 분명하지 않다면 나중에 추가할 수 있음) 이는 이벤트들이 촉매제가 재가열되는 동안의 폭주(runaway) 반응을 가리키고 있기 때문이다. 사고를 설명할 필요가 없는 경우라면 나중에 제거할 수 있고 이 시점에서 생략하면 나중에 추가할 수 있다. 컨트롤 스트럭처가 분석을 가이드하고 누락된 원인 분석을 쉽게 식별할 수 있도록 하지만, 주요 용도는 최종 보고서에서 사고에 대한 일관된 설명, 발생 이유, 그리고 변경해야할 사항을 제공하는 데 도움을 주는 것이다.

설계 활동에 대한 책임은 어딘가에 있다; 쉘 뫼르딕의 경우 지역 설계 그룹에서 플랜트를 설계하며(그림 14에는 표시되지 않지만 플랜트 관리의 일부이며 그 컨트롤 하에 있다고 여겨짐), 쉘 프로젝트 앤 테크놀로지(Shell Projects and Technology)가 글로벌 수준에서 감독하거나 검토한다. 또한 기업이나 글로벌 수준에서 항상 몇 가지 형태의 안전 관리가 존재한다. 마지막으로 경영진(최소한 이사회 정도)은 거의 항상 기업 경영 수준에서 몇 가지 유형의 기업 책임 및 안전에 대한 감독을 가지고 있다. 여기서 컨트롤 스트럭처는 다음과 같다.

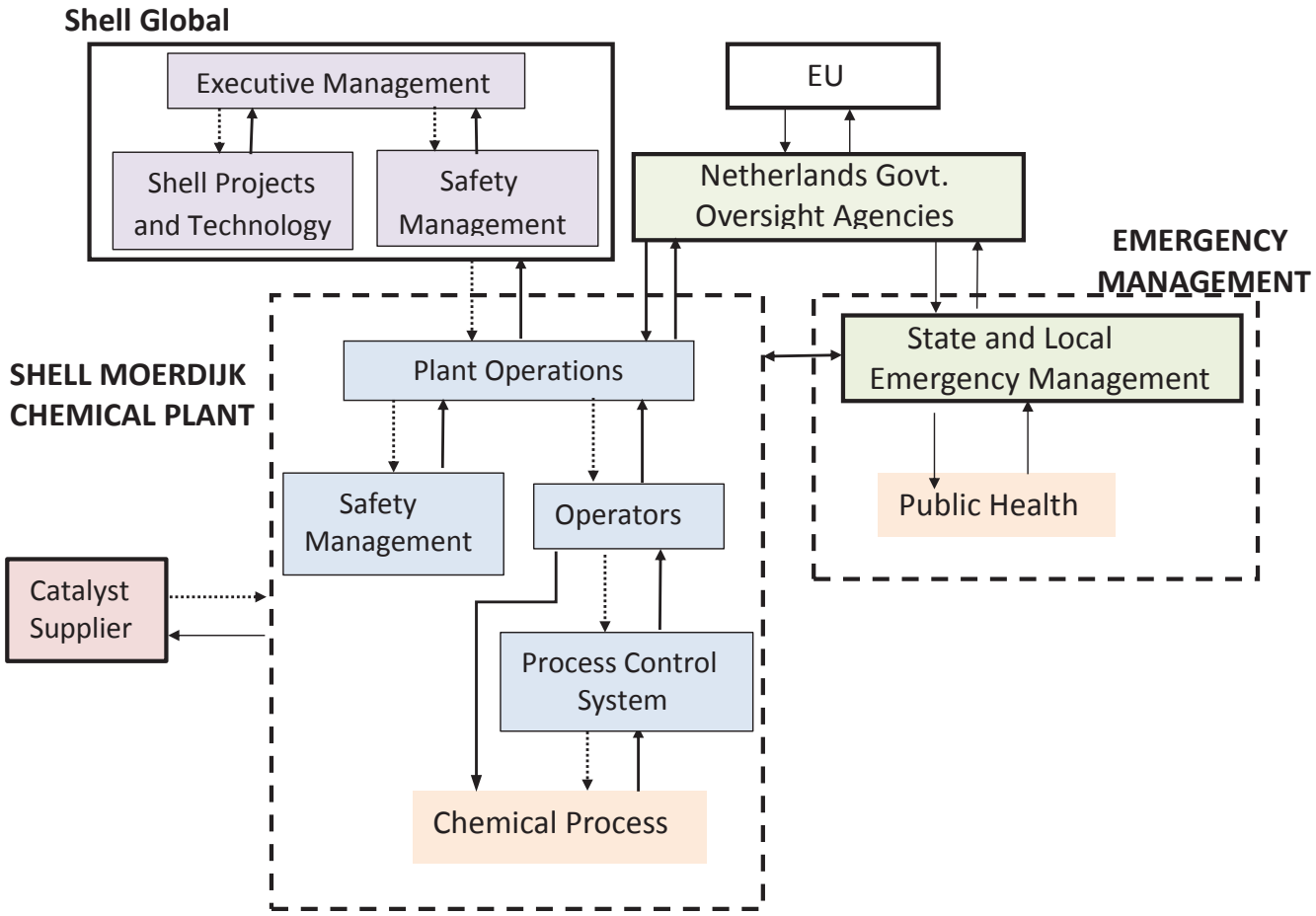



**Figure 14**: Shell Moerdijk safety control structure with more detail.

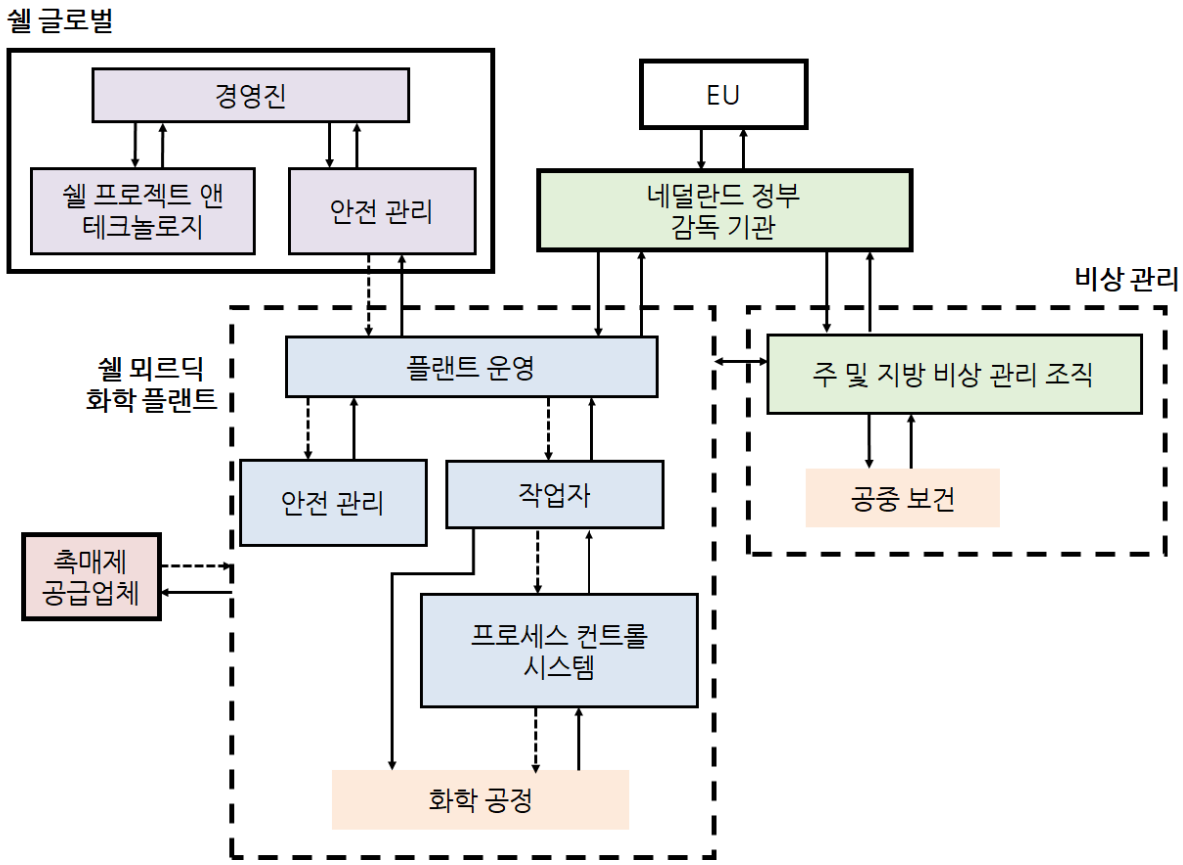



그림 14: 보다 상세한 쉘 뫼르딕(Shell Moerdijk) 안전 컨트롤 스트럭처

For readers who are familiar with STPA, which also starts with modeling the control structure, the model used in CAST need not be as detailed as that needed to perform STPA. In using CAST, most of the details will be filled in as the analysis proceeds. But the basic components should be identified at the beginning to help guide the analysis.

Once the basic components are identified, a specification of the responsibilities of each component can be started. For example, here are the responsibilities for the components included so far in the Shell Moerdijk safety control structure (Figure 14):

Process Control System safety-related responsibilities:

- Assist operators in controlling the plant during normal production and off-nominal operations (shut down, startup, maintenance, emergencies, etc.).
- Display relevant values, provide alerts, issue control actions on plant equipment.
- Control temperature, pressure, level, and flow to ensure that the process remains within the safe margins and does not end up in an alarm situation.

Operator Responsibilities:

General:

- Operate the plant in a way that does not lead to hazards
  - Monitor plant conditions and alarms
  - Control the process so that that it stays within safe boundaries of operation
  - Respond to unsafe conditions that occur.

Specific to this accident:

- Adjust gas and liquid flows as needed during startup.
- Make sure the Unit is not heated too quickly (in part to prevent damage to the catalyst pellets).

Plant Safety Management Relevant Responsibilities

- Identify plant hazards and ensure that they are eliminated, mitigated, or controlled.
- Either provide work instructions for safety-critical activities or review the work instructions provided by someone else for their safety implications.
- Ensure appropriately trained, skilled, and experienced people are assigned to high risk processes.
- Follow the Management of Change (MOC) procedures by doing a risk assessment for changes and implement risk controls based on the results.
- Provide for emergency treatment to exposed or injured individuals and ensure required medical equipment and personnel is available at all times. [*The injured personnel were treated effectively on the scene, so this aspect is not considered further.*]
- Perform audits of safety-critical activities or assist plant operations management in performing such audits [*It is not clear from the accident report who is responsible for audits, but there do appear to have been audits.*]

Operations Management relevant Safety-Related Responsibilities

- Establish safety policy for operations
- Ensure that Safety Management is fulfilling their responsibilities and providing realistic risk and hazard assessments.
- Use the results of the hazard and risk analyses provided by Safety Management in decision making about plant operations.

STPA에 익숙한 독자가 컨트롤 스트럭처 모델링을 시작하는 경우에 CAST에 사용되는 모델은 STPA에서 필요한 만큼 상세할 필요는 없다. CAST 사용 시 분석이 진행됨에 따라 세부사항의 대부분이 채워질 것이다. 그러나 처음에는 분석을 가이드하기 위해 기본적인 컴포넌트를 식별하여야 한다.

기본 컴포넌트가 식별되면 각 컴포넌트 책임에 대한 명세를 시작할 수 있다. 예를 들어 지금까지 쉘 뫼르딕 안전 컨트롤 스트럭처에 포함된 컴포넌트에 대한 책임은 다음과 같다. (그림 14):

프로세스 컨트롤 시스템의 안전 관련 책임:

- 정상적인 생산 및 비정상적인 작업(셧다운, 기동, 유지보수, 비상상황 등) 중 플랜트를 컨트롤할 수 있도록 운영자를 지원한다.
- 관련 수치를 표시하고 경고를 제공하며 플랜트 장비에 대한 컨트롤 액션을 실시한다.
- 온도, 압력, 레벨, 유량을 컨트롤하여 프로세스가 안전한 범위 내에서 유지되고 경보 상황이 발생하지 않도록 한다.

운영자의 책임:

일반 책임:

- 위험을 유발하지 않는 방식으로 플랜트를 운영한다.
  - 플랜트의 상태와 경보를 모니터링 함
  - 안전한 작동 범위 내에서 동작하도록 프로세스를 컨트롤함
  - 안전하지 않은 상황에 대응함

이 사고에 대한 구체적 책임:

- 기동 중에 필요에 따라 가스 및 액체 유량을 조정한다.
- Unit이 너무 빨리 가열되지 않도록 한다(촉매제 펠릿의 손상을 방지하기 위해).

플랜트 안전 관리 관련 책임

- 플랜트 위험을 파악하고 제거, 완화 또는 컨트롤되는지 확인한다.
- 안전 중요 활동에 대한 작업 지침을 제공하거나 다른 사람이 제공한 작업 지침을 검토하여 안전에 미치는 영향을 파악한다.
- 충분히 훈련되었고 숙련되었으며 경험이 풍부한 사람을 리스크가 높은 프로세스에 배정한다.
- 변경 사항에 대한 리스크 평가를 수행하여 변경관리(MOC) 절차를 따르고, 그 결과에 기반하여 리스크 컨트롤을 구현한다.
- 노출되거나 부상당한 사람에게 응급 처치를 제공하고 필요한 의료 장비 및 인력이 항상 가용하도록 보장한다. [부상자는 현장에서 충분히 치료되었으므로 이 측면은 더 이상 고려되지 않음]
- 안전 중요 활동을 감사(audit)하거나 그러한 감사 수행 시 플랜트 운영 관리를 지원한다. [사고 보고서 상에는 누가 감사를 담당했는지 명확히 명시되어 있지 않지만 감사를 받은 것으로 보임]

운영 관리와 관련된 안전 관련 책임

- 작업을 위한 안전 정책을 수립한다.
- 안전 관리 조직이 책임을 이행하고 현실적인 리스크 및 위험 평가를 제공하도록 한다.
- 안전 관리 조직에서 제공하는 위험 및 리스크 분석 결과를 플랜트 운영에 대한 의사결정에 활용한다.

- Create a Shell Moerdijk Safety Management System consistent with the overall Shell Global Safety Management System and make sure it is both effective and being followed.

More specific operations management safety-related responsibilities include the following:

- Provide appropriate training for operators for nominal and off-nominal work activities.
- Follow MOC (Management of Change] procedures that require performing a risk assessment for changes or ensure that safety management is doing so. Use the risk assessment to provide oversight of the process and to design and implement risk controls in the plant and the operating procedures.
- Prepare (or at least review) the work instructions. Ensure they are safe and are being followed.
- Minimize number of personnel in the vicinity (at risk) during high-risk operations, such as a turnaround
- Keep records of incidents and lessons learned and ensure they are communicated and used by those that need to learn from them.
- Provide personnel assignments that are commensurate with the experience and training required for the activity.
- Provide a process control system that can assist operators in performing critical activities.
- Conduct audits. Establish leading indicators to be used in the audits (and in other feedback sources) or ensure that safety engineering is identifying appropriate leading indicators.

Shell Corporate Projects and Technology (Engineering) Safety-Related Responsibilities

- Create a safe design: Perform hazard analysis (or use the results of hazard analysis created by another group) and eliminate or mitigate the hazards in the design.
- Provide design, hazard, and operating information to the plant operators to assist those who are operating the plants in avoiding any hazardous scenarios that the designers were not able to eliminate or adequately mitigate in the design itself.
- Learn from the operation of their designs and improve the designs based on this feedback.

Shell Corporate Safety Management Relevant Responsibilities

- Safety of plant design, including conduct of hazard analysis on designs licensed to subsidiaries.
- Oversight of operational safety at the various Shell plants and facilities.
- Management of change procedures related to safety: creating them, making sure they are followed, and improving them using feedback from incidents.
- Communication among separate plants in different parts of the world about incidents, lessons learned, etc.
- Creating and updating a Shell-wide Safety Information System and ensuring the information is being communicated adequately both within Shell Corporate and globally and that it is complete and usable.

Executive-Level Corporate Management Responsibilities:

- Ensure that measures are taken to
  - Prevent major accidents from occurring and,
  - If accidents do occur, mitigating their consequences for humans and the environment
- Ensure the health and safety of the employees in relation to all aspects associated with the work (based on the Working Conditions Act and other regulations)
- Follow the government regulations in the countries where their plants are located.
- Create an effective safety management system and establish a strong safety culture policy. Ensure that the SMS and safety policies are being followed and they are effective.

- 쉘 글로벌 안전 관리 시스템과 동일한 쉘 뫼르딕 안전 관리 시스템을 구축하여 효과적으로 운영하고 따르도록 한다.

운영 관리의 보다 구체적인 안전 관련 책임은 다음과 같다:

- 운영자에게 정상적인 활동 및 비정상적인 활동에 대한 적절한 훈련을 제공한다.
- 변경사항에 대한 리스크 평가를 요구하는 MOC(변경관리) 절차를 준수하거나 안전 관리가 그렇게 하고 있는지 확인한다. 리스크 평가를 활용하여 프로세스를 감독하고 플랜트 및 운영 절차에서의 리스크 컨트롤을 설계하고 구현한다.
- 작업 지침을 준비(또는 최소한 검토)한다. 그 지침이 안전하며 준수되는지 확인한다.
- 턴어라운드 과정과 같이 리스크가 높은 작업 중에는 주변(리스크 부근) 인원을 최소화한다.
- 사건 및 교훈에 대한 기록을 유지하여 그것들로부터 학습해야 하는 사람들에게 전달하여 활용되도록 한다.
- 활동에 필요한 경험과 훈련을 갖춘 인력을 할당한다.
- 작업자들의 중요 활동 수행을 지원하는 프로세스 컨트롤 시스템을 제공한다.
- 감사를 실시한다. 감사(및 다른 피드백 소스)에 사용할 선행지표를 선정하거나 안전 엔지니어링에서 적절한 선행지표를 식별하였는지 확인한다.

<u>쉘 기업 프로젝트 앤 테크놀로지(엔지니어링)의 안전-관련 책임</u>

- 안전한 설계 생성: 위험 분석을 수행하고(또는 다른 그룹이 만든 위험 분석 결과를 활용하고) 설계 위험 요소를 제거하거나 완화한다.
- 설계자가 설계 단계에서 제거하거나 적절히 완화할 수 없었던 위험한 시나리오를 플랜트 운영자가 피할 수 있도록 지원하기 위해 설계, 위험 및 운영 정보를 제공한다.
- 그들의 설계에 기반한 운영으로부터 학습하고 이 피드백을 바탕으로 설계를 개선한다.

<u>쉘 기업의 안전 관리에 관련된 책임</u>

- 자회사에 라이선스를 준 설계에 대한 위험분석 수행을 포함한 플랜트 설계 안전
- 다양한 쉘 플랜트 및 시설에서의 운영 안전을 감독한다.
- 안전과 관련된 변경절차 관리: 변경절차를 만들고 그 절차를 준수하는지 확인하며 사건으로부터의 피드백을 통해 변경절차를 개선한다.
- 사건, 교훈 등에 대해 세계 각지의 플랜트 간에 의사소통을 수행한다.
- 광범위한 쉘 안전 정보 시스템을 구축하고 업데이트하여 그 정보가 쉘 기업 및 전 세계적으로 적절히 전달되게 하고, 완전하며 사용 가능하도록 한다.

<u>임원의 기업 관리 책임</u>:

- 다음을 위한 조치가 취해지도록 한다.
  - 중대한 사고 발생을 방지하고,
  - 사고가 발생한 경우에는 사람과 환경에 미치는 영향을 완화함
- 업무의 모든 측면과 관련된 직원의 건강 및 안전을 보장한다.(근로조건법 및 기타 규정에 따라)
- 플랜트가 위치한 국가의 정부 규정을 준수한다.
- 효과적인 안전 관리 시스템(SMS)을 구축하고 강력한 안전 문화 정책을 수립한다. SMS 및 안전 정책이 준수되고 있고 효과적인지 확인한다.

Catalyst Manufacturer Safety-Related Responsibilities

- Provide information to customers necessary to evaluate the use of their catalyst in the reactor being designed and/or operated
- Alert customers when changes are made in the catalyst that could potentially affect the safety of its use.

Dutch Regulatory Authorities

All Dutch oversight safety and environmental authorities are grouped together here.

There are two main policies underlying this regulatory oversight:

1. Brzo: Companies must take all measures to prevent accidents and, if they occur, mitigate their consequences for humans and the environment. The company must implement this obligation by laying down policy assumptions in the Prevention Policy for Serious Accidents (PBZO), drawing up a safety report (VR), and organizing a safety management system.
2. Wabo: Regulators must check whether the company complies with regulations connected to the environmental permit, i.e., environmental safety.

*General Relevant Safety-Related Responsibilities*:

- Responsible for supervision and enforcement of Dutch laws to protect the environment and the public. Perform Brzo inspections focusing on process safety and Wabo inspections focusing on environmental safety.
- Responsible for enforcement of EU health and safety laws within the Netherlands.

*More Specific Responsibilities*:

- Identify shortcomings at companies they are responsible to oversee.
- Encourage companies to improve their safety-critical processes through supervision and enforcement. Identify shortcomings and persistently question companies to prompt them to investigate and detect deep-seated causes of incidents and accidents. Ensure that any shortcomings identified are corrected.
- Assess modifications made to plants, procedures, and processes (although they are not expected to perform the risk analyses for the companies).
- Pay greatest attention to safety-critical processes, including maintenance and reactor start-up

Emergency Services Responsibilities

- Firefighting, crisis management, crisis communications including among other things:
  - Informing citizens of the incident,
  - Measuring substances released on a coordinated basis,
  - Operating a telephone advisory line,
  - Informing citizens about the results of the measurement of the substances released and the ensuing recommendations.

Again, the control structure model is not fixed but can and most likely will evolve and change as more is learned about the accident and about the responsibilities of each of the control structure components. The CAST analysis will essentially involve identifying whether the responsibilities were effectively implemented and, if not, why not and what changes might be made to prevent this type of accident in the future. Another potential conclusion might be that responsibilities are not adequately identified or

촉매제 제조업체의 안전 관련 책임

- 설계 및/또는 운영 중인 반응로에서의 촉매제 사용을 평가하는 데 필요한 정보를 고객에게 제공한다.
- 촉매제의 사용 안전성에 잠재적 영향을 줄 수 있는 변경이 있는 경우 고객에게 경고한다.

네덜란드 규제 당국

모든 네덜란드의 안전 및 환경 감시 당국은 여기에 함께 그룹화 되어 있다.
이 규제 감독에는 두 가지 주요 정책이 있다:

1. Brzo(Besluit risico's zware ongevallen) : 회사는 사고를 방지하기 위한 모든 조치를 취해야 하고, 만약 사고가 발생하면 사람과 환경에 미치는 결과를 완화해야 한다. 회사는 심각한 사고 예방 정책(PBZO)에 대해 정책적 가정을 세우고 안전 보고서(VR)를 작성하며 안전 관리 시스템을 구성하여 이러한 의무를 이행해야 한다.
2. Wabo : 규제 기관은 회사가 환경 허가, 즉, 환경 안전과 관련된 규정을 준수하는지 확인해야 한다.

*일반적인 안전 관련 책임:*

- 환경과 공공을 보호하기 위해 네덜란드 법의 감독 및 집행에 책임이 있다. 프로세스 안전에 초점을 두고 있는 Brzo 검사와 환경 안전에 초점을 두고 있는 Wabo 검사를 수행한다.
- 네덜란드 내 EU 보건 및 안전 법률의 시행을 책임진다.

*보다 구체적인 책임:*

- 감독할 책임이 있는 회사의 결점(shortcoming)을 식별한다.
- 감독과 이행을 통해 기업이 안전 중요 프로세스를 개선하도록 독려한다. 결점을 식별하고 지속적으로 기업에 질의하여 사건 및 사고의 심층적 원인을 조사 및 탐지하도록 한다. 식별된 결점이 모두 수정되었는지 확인한다.
- 플랜트, 절차 및 프로세스에 대한 수정 사항을 평가한다(회사에 대한 위험 분석은 수행하지 않더라도).
- 유지보수, 반응로 기동(startup) 등 안전-중요 프로세스에 최대한 주의한다.

비상 서비스 조직의 책임

- 소방, 위기 관리, 아래 사항을 포함하는 위기 커뮤니케이션:
  - 시민들에게 사건 알림
  - 조정된 기준에 근거하여 유출된 물질 측정
  - 전화 상담 라인 운영
  - 유출된 물질의 측정 결과 및 후속 권고사항에 대해 시민들에게 알림

다시 말하지만, 컨트롤 스트럭처 모델은 고정되어 있지 않고 사고 및 컨트롤 스트럭처의 각 컴포넌트 책임에 대해 더 알게 될수록 진화하고 변경될 수 있다. CAST 분석에는 기본적으로 책임이 효과적으로 이행되었는지 여부, 그렇지 않다면 왜 그렇지 않은지, 그리고 미래에 이러한 유형의 사고를 예방하기 위해 어떤 변경이 이루어 질 수 있는지를 파악하는 것이 포함된다. 책임이 적절하게 식별되지 않거나 할당되지 않아 기본 안전 컨트롤 스트럭처가 재설계되어야 한다는 또 다른 잠재적인 결론에 이를 수도 있다. 대부분의 사고 조사에서 손실에 기여하는 이 유형을 모두 발견할 것이다.

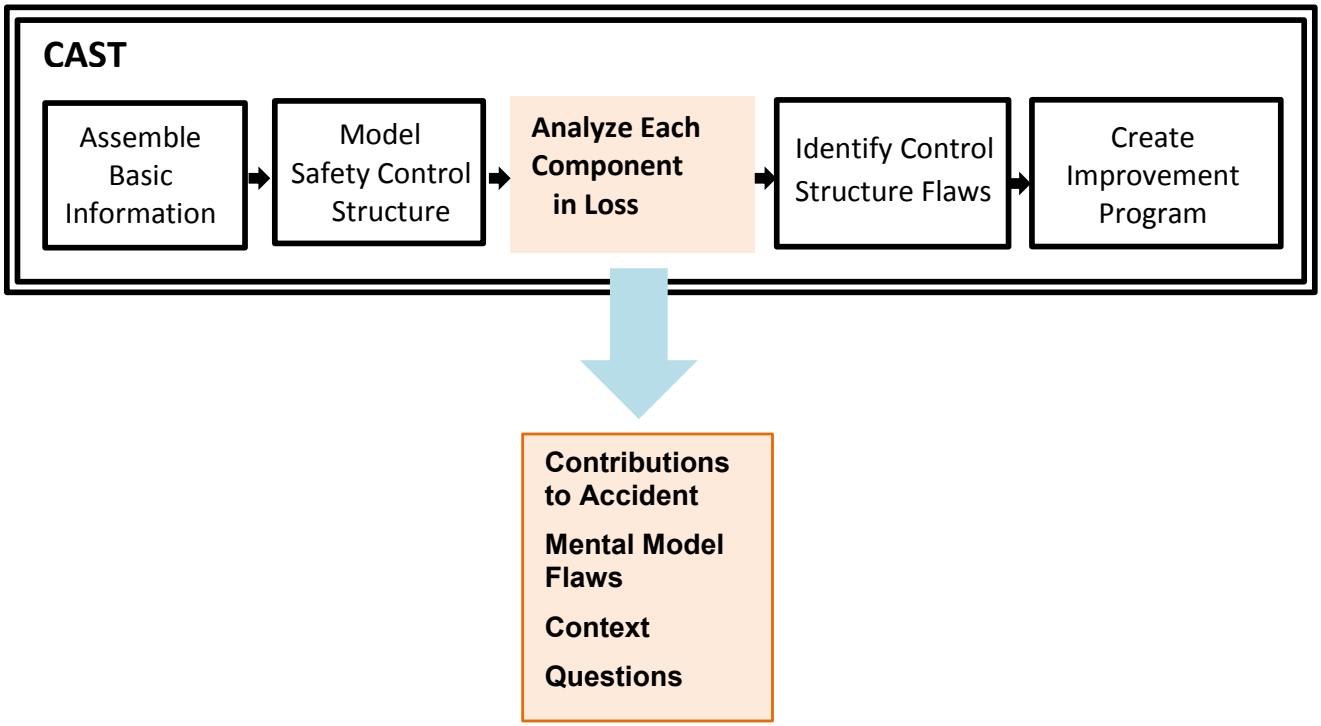
분석하는 사람들은 책임을 어떻게 식별할까? 대부분의 책임은 회사 매뉴얼이나 정부 문서에 기록되

appropriately assigned and that the basic safety control structure needs to be redesigned. Most accident investigations will likely find both types of contributors to the loss.

How does the analyst identify the responsibilities? Most of these will be documented somewhere, either in company manuals or government documents. In addition, questioning the controllers about their own and other's responsibilities during the investigation will at least elicit what the controllers think they are. Confusion and inconsistencies here could be a clue as to why the accident occurred. One of the important characteristics of the U.S. Navy's SUBSAFE program, which has been spectacularly successful over its 50+ year existence, is that everyone in the program knows exactly what are their own responsibilities and also what everyone else's are. By continually reinforcing and auditing this knowledge about responsibilities, accidents are reduced.

어 있을 것이다. 또한 조사 과정에서 컨트롤러 및 다른 컨트롤러들의 책임에 대한 질문을 통해 적어도 컨트롤러가 인지하고 있는 것들을 이끌어 낼 수 있을 것이다. 여기서의 혼동과 불일치가 사고 발생 이유에 대한 단서가 될 수 있다. 50년 이상 극적인 성공을 거둔 미 해군 SUBSAFE 프로그램의 중요한 특징 중 하나는, 이 프로그램에 참여한 모든 사람들이 자신의 책임뿐만 아니라 다른 모든 사람들의 책임을 정확히 알고 있다는 것이다. 책임에 대한 인식을 지속적으로 강화하고 감사(audit)함으로써 사고는 줄어든다.

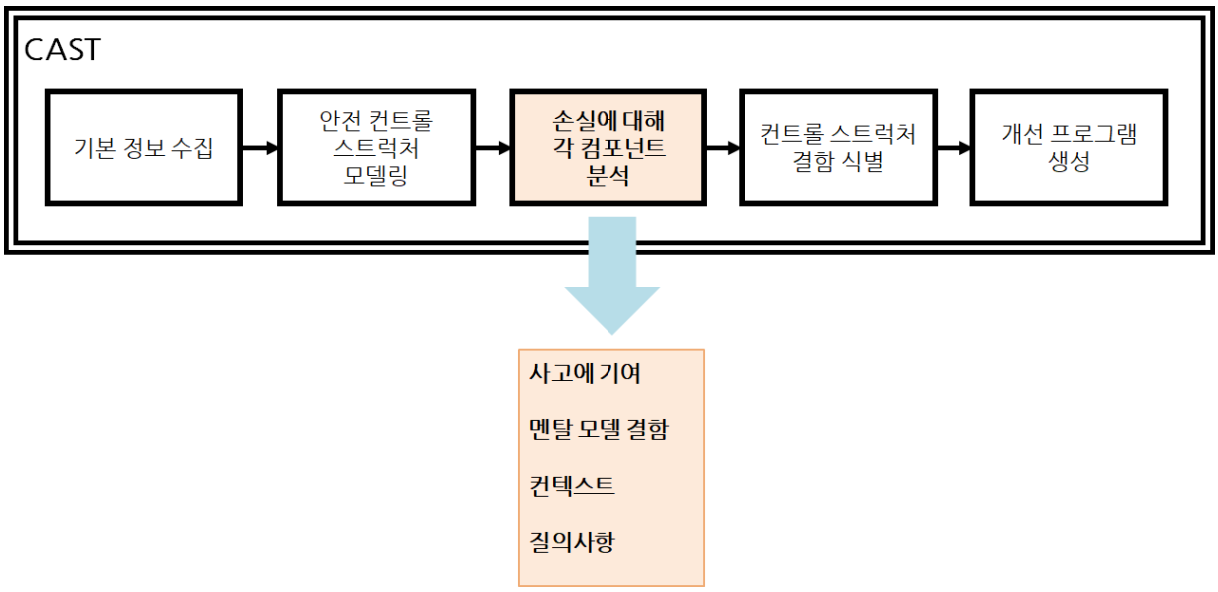
## Individual Component Analysis: Why were the Controls Ineffective?




3. *Examine the components of the control structure to determine why they were not effective in preventing the loss:*

   *Starting at the bottom of the control structure, show the role each controller played in the accident and the explanation for its behavior: why each control component did what it did and why the controller thought it was the right thing to do at the time.*

## 개별 컴포넌트 분석 : 컨트롤이 왜 효과가 없었는가?




*3. 컨트롤 스트럭처의 컴포넌트를 조사하여 손실 방지에 효과가 없었던 이유를 파악한다:*

*컨트롤 스트럭처의 가장 아래에서 시작하여 사고에서 각 컴포넌트가 수행한 역할과 동작에 대한 설명(그들이 한 일과 그 당시에 왜 옳은 일이라고 생각했는지)을 제시한다.*

Once the basic control structure and controls are identified, the next step is to show why the control structure, i.e., the current controls, did not prevent the accident. There will be two parts to this process. The first, described in this section, looks at the individual controllers (which may be automated or human) and the role they played in the accident. The second, described in the next section, looks at the operation of the control structure as a whole and the interactions among the components. Remember, the goal is to identify flaws in the control structure: not to assign blame to individuals or individual components but to understand why it made sense for them to act the way they did.

Also, as started in the previous steps, the CAST process includes generating questions that need to be answered during the investigation so that at the end, a complete explanation for why the accident occurred can be provided. I find it most helpful to start at the bottom components in the control structure and work my way upward.

There are several parts in the CAST analysis of each controller:

- Component responsibilities related to the accident
- Contribution (actions, lack of actions, decisions) to the hazardous state: [16]

*Why?*

- Flaws in the mental/process model contributing to the actions:
- Contextual factors explaining the actions, decisions, and process model flaws:

The first two parts simply document the role the component played in the loss, if any. The component safety-related responsibilities were identified when modeling the safety control structure. Only those related to the loss need to be considered. The role or contribution (behavior related to the hazardous state) will be the responsibilities that were not fulfilled. For example, one responsibility of the operators during reheating of the reactor at Shell Moerdijk after a maintenance stop is to control the process so that it stays within safe boundaries of operation. In this case, they did not adjust the gas and liquid flows in a way that prevented the overheating of the catalyst pellets. Remember, no judgmental or hindsight words should be used like they "failed" to adjust the flows or they "should have" adjusted the flows. Simply describe what happened in a non-accusatory way. The behavior that contributed to the loss is described in a straightforward manner that simply says what the person or group did or did not do.

The "why" part of the analysis involves explaining why the component behaved in the way it did, i.e., the contextual and other factors that made the behavior seem correct to them at the time. For example, contextual factors might include incorrect information that the controller had at the time, inadequate training, pressures and incentives to act the way they did, misunderstanding about their role or about how the controlled components worked, etc. This "why" part of the analysis will also involve answering the questions previously raised about the behavior of this component. Answering the "why" questions for a component usually raises more questions, which may need to be answered in the analysis of the higher levels of the control structure. The goal is that at the end of the CAST analysis, all the questions raised are answered. In reality, there may be remaining questions that just cannot be answered definitively. These should, of course, be documented in the final conclusions. If the people involved understand that the goal of the accident investigation and causal analysis are not to find "guilty parties,"

[16] Although in STPA the term "unsafe control actions" is used without much complaint, the use there is about hypothetical actions and not things that actually have occurred. Using that term in CAST lends a tint of blame and judgment and should be avoided. We have used various terms such as "Control actions contributing to the hazard" or contributory control actions or simply "role or contribution of the controller to the hazardous state" to avoid common pejorative terminology.

기본 컨트롤 스트럭처 및 컨트롤이 식별되면 다음 단계는 컨트롤 스트럭처, 즉, 현재의 컨트롤이 사고를 방지하지 못한 이유를 보여주는 것이다. 이 프로세스에는 두 가지 파트가 있을 것이다. 이 섹션에서 설명하고 있는 첫 번째는 개별 컨트롤러(자동화 또는 사람일 수 있음)와 그 컨트롤러들이 사고에서 한 역할을 살펴보는 것이다. 두 번째는 컨트롤 스트럭처의 작동과 컴포넌트 간의 상호작용을 전체적으로 살펴보는 것이다. 컨트롤 스트럭처의 결함을 확인하는 것이 목표임을 기억해야 한다: 개인이나 개별 컴포넌트에 책임을 부여하는 것이 목표가 아니고 왜 그들이 그것을 타당하다고 생각하여 행동하였는지를 이해하는 것이다.

또한, 이전 단계와 같이 CAST 프로세스에는 조사 중에 답변해야 할 질문을 생성하는 단계가 포함되어 있으며 이를 통해 결과적으로 사고가 발생한 이유에 대해 완전한 설명을 제공할 수 있다. 저자는 컨트롤 스트럭처의 하위 컴포넌트에서 시작하여 위쪽으로 올라가는 것이 가장 유용하였다.

각 컨트롤러에 대한 CAST 분석에는 여러 부분이 있다:

- 사고와 관련된 컴포넌트의 책임
- 위험한 상태에 대한 기여 (행동, 행동의 결여, 의사결정):[16]

*왜(WHY)?*

- 행동의 원인이 되는 멘탈/프로세스 모델의 결함:
- 행동, 결정 및 프로세스 모델의 결함을 설명하는 컨텍스트적 요인:

앞의 두 가지는 단순히, 손실에 대해 컴포넌트가 수행한 역할이 있다면 이를 문서화한다. 안전 컨트롤 스트럭처를 모델링할 때 컴포넌트의 안전 관련 책임을 식별하였는데, 여기서 손실과 관련된 책임만을 고려하면 된다. 손실에 대한 컴포넌트의 역할이나 기여(위험한 상태와 관련된 동작)는 이행하지 않은 책임일 것이다. 예를 들어 쉘 뫼르딕의 반응로 재가열 과정에서 유지보수 중단 후의 운영자의 책임 중 하나는 프로세스를 컨트롤하여 프로세스가 안전한 작동 범위 내에 있도록 하는 것이다. 앞의 경우에서 운영자들이 촉매제 펠릿의 과열을 방지하는 방향으로 가스와 액체 유량을 조정하지 않았다. 그들이 유량 조정에 "실패했다" 또는 유량을 조정 "했어야 했다" 처럼 비판적이나 사후 확신적(hindsight) 단어를 사용해서는 안 된다는 것을 기억해야 한다. 비난적이지 않은 방식으로 단순히 무슨 일이 일어났는지를 설명하면 된다. 손실에 기여한 동작은 사람이나 그룹이 한 일 또는 하지 않은 일을 단순히 말하는, 복잡하지 않은 방식으로 설명된다.

분석의 "왜(Why)" 부분은 컴포넌트가 왜 그렇게 동작했는지, 즉, 컨텍스트적이거나 다른 요인이 당시에 그 동작을 올바른 것처럼 보이게 한 이유를 설명하는 것이다. 예를 들어 컨텍스트적 요인에는 당시 컨트롤러가 가지고 있던 잘못된 정보, 부적절한 훈련, 수행 방식에 대한 압박 및 장려, 역할 또는 제어되는 컴포넌트의 작동 방법에 대한 잘못된 이해 등이 포함될 수 있다. 분석의 "왜(Why)" 부분에는 이 컴포넌트의 동작에 제기된 질문에 대한 답변도 포함될 것이다. 컴포넌트에 대한 "왜(Why)" 라는 질문에 답하는 것은 일반적으로 더 많은 질문을 제기하게 하며 이는 컨트롤 스트럭처의 보다 상위 수준 분석에서 답변해야 할 수도 있다. CAST 분석이 끝날 때, 제기된 모든 질문에 대답하는 것이 목표이다. 그러나 실제로는 확실하게 대답할 수 없는 질문들이 남아 있을 수도 있다. 물론 최종 결론에는 대답하지 못한 질문들이 기록되어야 한다. 만약 사고와 관련된 사람들이 사고 조사 및 원인 분석의 목표가

16 STPA에서는 "안전하지 않은 컨트롤 액션(unsafe control action)"이라는 문구가 별다른 이견 없이 사용되는데, 여기서는 실제로 발생했던 액션이 아니라 가정된 액션에 대해 사용한다. CAST에서 그 용어를 사용하는 것은 비난 및 판단의 의미를 나타내므로 해당 용어의 사용을 피해야 한다. 우리는 흔한 비난적인 용어의 사용을 피하기 위해 "위험에 기여하는 컨트롤 액션"이나 원인이 되는 컨트롤 액션 또는 단순히 "위험한 상태에 대한 컨트롤러의 역할 또는 기여"와 같은 문구를 사용하고 있다.

they are more likely to provide candid answers. Enlist their help as part of an explanatory process to improve safety in the future. This kind of trust, of course, needs to be established over time.

Focus on understanding "why" the controllers acted the way they did. Most controllers are trying to do the right thing. If they had evil intent (were suicidal or homicidal), of course, that needs to be identified but such behavior is rare in accidents. Usually the controllers are trying to do a good job, and there is some reason that they didn't. For automated controllers, understanding will involve looking at the design and the designers of the automation and the assumptions they made about what type of behavior was required. Almost all software-related accidents involve incorrect assumptions about the behavior required to prevent the hazards, i.e., a flawed understanding of the requirements for safe operation.

Understanding the reasons for the behavior that occurred will provide the best guidance possible in creating effective recommendations. If the accident report identifies only what the controller did wrong, we learn almost nothing required to prevent the same behavior in the future beyond telling people "don't do that." As the controllers usually had a good reason for doing it at the time, this type of instruction is not helpful. Rules and procedures are never mindlessly obeyed under all circumstances. If the designers of the system intend for operators to thoughtlessly follow written directions, then those control responsibilities should be automated. Checklists are often provided as guidance, but we usually want people to make judgments about the appropriateness of the checklist at the time of the emergency. If they did not follow the checklist when they should have, then we need to understand why.

Humans are left in systems today to make cognitively complex decisions about what needs to be done. If they make the wrong decisions, the reasons why (e.g., they had incorrect information, they were misled by the process control system output, they were not given adequate support to make safe decisions, there was no or misleading feedback about the state of the component they were controlling) will provide the information needed to redesign the safety control structure and safety controls to assist controllers in making better decisions in the future.

The CAST process is designed to avoid hindsight bias as much as possible. After the accident or incident, the behavior will appear to be clearly wrong. That's obvious and doesn't need to be stated. What is useful is to understand why—*at that time*—it was not obviously wrong to the controller. Why not? What types of information did they need to make a better decision? Did they have it? Did they understand what that information meant at the time? Were there other competing pressures that made it difficult for them to absorb the information or to process it? The more fully the context can be identified, the more effective any resulting recommendations will be in reducing future losses. The context may be physical, psychological, informational, managerial, and situational, such as workload or productivity pressures, incentives/disincentives, etc.

The notation used to record the results of this analysis step is irrelevant as long as the information is recorded and easy to understand. Some suggestions for notations we have been used successfully are included at the end of this chapter.

In this handbook, only a few examples from the CAST analyses of the Shell Moerdijk are shown. A summary of the role played by all the components is provided in Appendix B. Links to the complete CAST analysis for Shell Moerdijk as well as many other real accidents are provided in Appendix A.

An automated process control system is a standard controller for plants. Therefore, it's a convenient place to start in understanding the Shell Moerdijk explosion. The safety-related responsibilities include:

Safety-Related Responsibilities of the Process Control System:

1. Assist operators in controlling the plant during normal production and off-nominal operations (shut down, startup, maintenance, emergencies, etc.).

"유죄 당사자"를 찾는 것이 아님을 이해한다면 보다 솔직한 답변을 할 수도 있다. 향후 안전을 개선하기 위한 설명 프로세스의 일환으로 그들의 도움을 요청해야 한다. 물론 시간이 지남에 따라 어느 정도의 신뢰가 형성될 필요가 있다.

컨트롤러가 "왜" 그런 방식으로 동작했는지를 이해하는 데 집중하라. 대부분의 컨트롤러는 옳은 것을 행하려고 한다. 물론 그들이 악의적인 의도(자살 또는 살인)를 가지고 있었다면 그에 대해서는 확인할 필요가 있지만 사고에서는 그러한 악의적인 동작은 아주 드물다. 일반적으로 컨트롤러는 일을 잘하려고 노력하고 있으며 그렇지 않은 경우에도 그럴만한 이유가 있다. 자동화된 컨트롤러의 경우 자동화 설계 및 설계자를 이해해야 하고 요구되는 동작 유형에 대한 가정도 이해해야 할 것이다. 거의 모든 소프트웨어 관련 사고는 위험 방지에 요구되는 동작에 대한 잘못된 가정, 즉, 안전한 운영 요구사항에 대한 잘못된 이해와 관련이 있다.

일어난 행동에 대한 이유를 이해하는 것은 효과적인 권고사항을 만드는 데 가장 좋은 지침이 될 것이다. 사고 보고서에 컨트롤러가 잘못 동작한 것만을 작성한다면, 우리는 사람들에게 '그렇게 행동하지 말 것'이라고 말하는 것 외에는 향후 같은 행동을 예방하기 위해 필요한 것을 거의 배우지 못한다. 컨트롤러들은 대개 그 당시에 그런 동작을 해야 할 충분한 이유가 있었기 때문에 이런 유형의 지침은 도움이 되지 않는다. 모든 상황에서 규칙과 절차가 무의식적으로 준수되는 것은 아니다. 만약 시스템 설계자들이 운영자로 하여금 생각 없이 서면 지시를 따르게 한다면 그러한 컨트롤 책임은 자동화해야 한다. 지침으로서 체크리스트가 종종 제공되지만 우리는 사람들이 비상시 체크리스트의 적절성을 스스로 판단하기를 원한다. 만약 그들이 체크리스트를 따라야 할 때 따르지 않았다면 그 이유를 이해할 필요가 있다.

오늘날 시스템에서 사람들은 무엇을 해야 하는지에 대해 인지적으로 복잡한 결정을 내린다. 만약 그들이 잘못된 결정을 내린다면 그 이유는(예를 들어 잘못된 정보를 가지고 있었거나, 프로세스 컨트롤 시스템 출력에 의해 호도되었거나, 안전한 결정을 내리기 위한 적절한 지원을 받지 못했거나, 그들이 컨트롤하고 있는 컴포넌트의 상태에 대한 피드백이 없었거나 잘못된 피드백이 있는 경우) 컨트롤러가 미래에 더 나은 결정을 내릴 수 있도록 안전 컨트롤 스트럭처와 안전 컨트롤을 재설계 하는 데 필요한 정보를 제공할 것이다.

CAST 프로세스는 가능하면 사후 확신 편향(hindsight bias)을 지양하도록 설계되었다. 사건 또는 사고 발생 후에는 동작이 분명 잘못된 것으로 보일 것이다. 그것은 명백하여 굳이 말할 필요도 없다. 도움이 되는 것은 *그 당시에* 컨트롤러에게 그것이 명백히 잘못된 것이 아닌 이유를 이해하는 것이다. 왜 그렇지 않았겠는가? 그들이 더 나은 결정을 내리기 위해서는 어떤 유형의 정보가 필요했을까? 그들이 그러한 정보를 가지고 있었는가? 그 당시 그들은 정보의 의미를 이해했는가? 정보를 받아들이거나 처리하기 어렵게 하는 다른 압박이 있었는가? 컨텍스트를 완전히 파악할수록 향후 손실을 줄이기 위한 보다 효과적인 권고사항이 도출될 것이다. 컨텍스트는 업무량 또는 생산성 압박, 장려사항/의욕저해사항 등과 같이 물리적, 심리적, 정보적, 관리적 그리고 환경적인 것일 수 있다.

이 분석 단계의 결과를 기록하는 표기법은 정보가 기록될 수 있고 이해하기 쉽다면 어떤 형태여도 무관하다. 이 장의 끝 부분에 우리가 성공적으로 사용한 몇 가지 표기법이 제시한다.

이 핸드북에서는 쉘 뫼르딕 CAST 분석에 대한 몇 가지 예시만 제시한다. 모든 컴포넌트의 역할에 대한 요약은 부록 B에서 볼 수 있다. 쉘 뫼르딕에 대한 CAST 전체 분석 링크및 다른 실 사고에 대한 링크는 부록 A에서 볼 수 있다.

자동화된 프로세스 컨트롤 시스템은 플랜트의 표준 컨트롤러이다. 따라서 쉘 뫼르딕 폭발에 대한 이해의 시작점으로 용이하다. 안전 관련 책임에는 다음과 같은 것들이 포함된다:

2. Display relevant values, provide alerts, issue control actions on plant equipment.
3. Control temperature, pressure, level, and flow to ensure that the process remains within the safe margins and does not end up in an alarm situation.

To identify its role in the loss, we can start with determining whether these responsibilities were satisfied. In this case, the process control system contributed to the accident by:

Contribution to the hazardous state:

1. The process control system did not provide the assistance required by the operators to safely control the start-up process, including automatically controlling the heating rate and other important variables.
2. The process control system did not step in to stop the process when pressure and temperature increased precipitously.
3. The process control system did not issue an automatic reset after two high-high level alarms, so the gas discharge system remained closed.

As an example of the detailed "why" analysis, i.e., the contextual factors for number 2 (i.e., the process control system did not stop the process when pressure and temperature increased precipitously), consider:

| Why? (Contextual Factors Affecting the Unsafe Control) | Questions Raised |
|---|---|
| There was no emergency stop button for Unit 4800. Without an emergency stop, there was no way to safely stop the operation of the unit quickly with a single press of a button. No reason was provided for this design "flaw" in the accident report but could have been answered at the time of the investigation. Emergency stop buttons are standard in safety-critical systems. | *Was this complacency, cost, or was there an engineering reason?* |
| The instrument-based safety devices were designed to respond to and prevent particular conditions, but not the ones that occurred. After this accident, a safety device was added to protect Unit 4800 from an excessively high temperature due to an unwanted chemical reaction with hydrogen. | *Why were these conditions omitted? Was a hazard analysis performed that could have identified them?* |
| There is a containment system, which is described as "one or more appliances of which any components remain permanently in open connection with each other and which is/are intended to contain one or more substances." The valves of the containment system, however, cannot be remotely operated and must be operated manually. Due to the intensity of the fire that night and the risk of additional explosions, it was not possible for these valves to be operated immediately and, in fact, were not operated until several hours later when the fire had been extinguished. | *The containment system design was not useful in this situation. Was this known beforehand? Was it impossible to design one that can be operated remotely?* |

프로세스 컨트롤 시스템의 안전 관련 책임:

1. 정상적인 생산 및 비정상적인 작업(셧다운, 기동, 유지보수, 비상상황 등) 중 작업자가 플랜트를 컨트롤할 수 있도록 지원한다.
2. 관련된 수치를 표시하고 경보를 제공하며 플랜트 장비에 컨트롤 액션을 제공한다.
3. 프로세스가 안전한 범위 내에서 유지되고 경보 상황에 빠지지 않도록 온도, 압력, 레벨 및 유량을 컨트롤한다.

손실에서 프로세스 컨트롤 시스템의 역할을 확인하기 위해 우리는 이러한 책임들이 만족되었는지를 파악하는 것부터 시작할 수 있다. 이 예제의 경우 프로세스 컨트롤 시스템은 다음과 같이 사고에 기여하였다.

위험한 상태에 대한 기여:

1. 프로세스 컨트롤 시스템이 가열 속도 및 기타 중요한 변수의 자동 제어 등을 포함하여, 작업자가 기동 프로세스를 안전하게 제어하는 데 필요한 지원을 제공하지 않았다.
2. 프로세스 컨트롤 시스템이 압력과 온도가 급격히 증가했을 때 프로세스를 중단시키기 위한 개입을 하지 않았다.
3. 두 번의 높은(high-high) 수준의 경보 후에도 프로세스 컨트롤 시스템이 자동 리셋 명령을 제공하지 않았고, 그래서 가스 배출 시스템이 닫힌 채로 유지되었다.

상세한 "이유(Why)" 분석의 예로서, 즉, 2번에 대한 컨텍스트적 요인(즉, 프로세스 컨트롤 시스템이 압력과 온도가 급격히 증가했을 때 프로세스를 중단시키지 않음)을 고려해 보자:

| **왜? (안전하지 않은 컨트롤에 영향을 미치는 컨텍스트적 요인)** | **제기된 질문** |
|---|---|
| Unit 4800에 비상 정지 버튼이 없었다. 비상 정지 없이는 한 번의 버튼 누름만으로 장치 운영을 신속하고 안전하게 중단시킬 방법이 없다. 사고 보고서에는 이러한 설계 "결함"에 대한 이유가 제시되지 않았지만 조사 과정에서 답변을 받을 수 있었다. 비상 정지 버튼은 안전-중요 시스템의 표준이다. | 안일함(complacency), 비용 또는 엔지니어링적인 이유였을까? |
| 그 기계 기반의 안전장치는 특정 조건을 반응 및 방지하기 위해 설계되었지만, 발생한 것은 그 특정 조건이 아니었다. 이 사고 이후, 수소와의 원치 않는 화학 반응으로 인한 지나치게 높은 온도로부터 Unit 4800을 보호하는 안전장치가 추가되었다. | 왜 이러한 조건들이 누락되었는가? 조건들을 파악할 수도 있었을 위험 분석이 수행되었는가? |
| "컴포넌트 간 연결(open connection)을 영구적으로 유지할 수 있고 하나 이상의 물질을 담을 수 있도록 고안된 하나 이상의 기기"라고 기술되는 격납 시스템이 있다. 그러나 격납 시스템의 밸브는 원격으로 작동할 수 없으며 수동으로 작동해야 한다. 그날 밤의 화재 강도(intensity)와 추가 폭발 리스크로 인해 이 밸브를 즉시 작동시킬 수 없었고 실제로 화재가 진압된 몇 시간 후까지 작동되지 않았다. | 격납 시스템의 설계는 이 상황에서 유용하지 않았다. 이 사실이 미리 알려져 있었는가? 원격으로 작동할 수 있는 시스템을 설계하는 것이 불가능했을까? |

An important part of the understanding of why a controller behaved the way it did may arise from an incorrect process/mental model. The CAST analysis involves both identifying the flaws in this model and determining why they occurred.

Process Control System Process Model flaws: The Shell Moerdijk process control system, for the most part, had correct information about the state of the process. There was some missing information about temperature, however, resulting from an inadequate number of temperature sensors provided in the reactors.

When the component analysis has been completed and documented (details not included here), a summary can be made of the role of the component in the accident along with recommendations. Any open questions that are important in the causal analysis should also be documented.

Summary of the Role that the Process Control System Played in the Accident: The process control system was not designed to provide the necessary help to the operators during a start-up or to allow them to easily stop the process in an emergency. The reason for these design decisions rests primarily in incorrect assumptions by the designers about the impossibility of the scenario that occurred. Even after previous incidents at similar plants in which these assumptions were violated, the assumptions were not questioned and revisited (see the CAST analysis of the safety information system).

More generally, the process control system was configured only for the normal production phase. There were no special automated control circuits for the heating phase after a catalyst has been replaced, which is the phase in which the problems arose. In fact, this phase is commonly known to be the most accident prone, so the decision not to provide automated help to the human operators during this phase is quite strange, but no explanation is provided in the accident report.

Unanswered questions: Why was a decision made not to provide assistance to the operators during the restart phase of operations? Why was an emergency stop capability not designed into the system?

Recommendations: The operators' knowledge and skill are most challenged during off-nominal phases, and most accidents occur during such phases and after changes are made or occur. The process control system should be redesigned to assist operators in all safety-critical, off-nominal operations (not just this restart scenario). For manual operations, the goal should be for the process control system to provide all necessary assistance to the operators in decision making and taking action and to reduce attention and time pressures (see the section on the operators).

The rest of this section shows examples from the Shell Moerdijk CAST analysis for different types of controllers. The process control system analysis provides an example of an automated controller. The other controllers for the Shell Moerdijk Chemical Plant were people or groups of people. Details, again, are omitted here for space reasons.

컨트롤러가 왜 그렇게 동작했는지를 이해하는 데 중요한 것은 잘못된 프로세스/멘탈 모델에서 찾을 수 있다. CAST 분석에는 이러한 모델의 결함을 식별하고 그 원인을 파악하는 것이 포함된다.

프로세스 컨트롤 시스템의 프로세스 모델 결함(flaws): 쉘 뫼르딕 프로세스 컨트롤 시스템은 대부분 프로세스 상태에 대한 정확한 정보를 가지고 있었다. 그러나 반응로의 온도 센서 개수가 부족하여 온도에 대한 정보가 누락되었다.

컴포넌트 분석이 완료되고 문서화되면(자세한 내용은 여기에 포함하지 않음) 사고에서의 컴포넌트 역할과 권고사항을 정리할 수 있다. 원인 분석에 있어서 중요하지만 답변되지 않은 질문(open question)도 문서화해야 한다.

사고에서의 프로세스 컨트롤 시스템 역할 요약: 프로세스 컨트롤 시스템은 기동(start-up) 중에 작업자에게 필요한 도움을 제공하거나 비상상황에서 프로세스를 쉽게 중지할 수 있도록 설계되지 않았다. 이러한 설계 결정의 주된 이유는 설계자들이 시나리오의 발생이 불가능하다고 잘못 가정한 것에 있다. 과거에 유사한 플랜트에서 이러한 가정이 위반된 사건이 발생한 후에도 가정에 대한 의문이 제기되거나 재검토되지 않았다(안전 정보 시스템에 대한 CAST 분석 참조).

보다 일반적으로는, 프로세스 컨트롤 시스템이 정상적인 생산 단계를 위해서만 구성되었다. 촉매제 교체 후의 가열 단계에 대한 특수 자동 제어 회로가 없었고 이 단계에서 문제가 발생하였다. 실제로 이 단계는 일반적으로 사고가 가장 발생하기 쉬운 것으로 알려져 있었기 때문에 이 단계에서 작업자에게 자동화된 도움을 제공하지 않기로 한 결정은 매우 의문스러웠지만 사고 보고서에는 그에 대한 설명이 없었다.

답변되지 않은 질문: 작업의 재구동 단계에서 작업자에게 지원을 하지 않기로 결정한 이유는 무엇인가? 비상 정지 기능이 시스템에 설계되지 않은 이유는 무엇인가?

권고사항: 비정상적(off-nominal) 단계에서의 운영자의 지식과 기술은 가장 중요하며 대부분의 사고는 그러한 단계에서, 변경이 이루어지거나 변경이 발생한 이후에 일어난다. 프로세스 컨트롤 시스템은 모든 안전-중요 작업, 비정상적 작업(단지 이번 재구동 시나리오뿐만 아니라)에서 운영자를 지원하기 위해 재설계되어야 한다. 수동 조작의 경우 목표는, 프로세스 컨트롤 시스템이 작업자의 의사 결정 및 조치에 필요한 모든 지원을 제공하고 주의력 및 시간 압박을 낮추어주는 것이어야 한다(작업자 섹션 참조).

이 섹션 나머지 부분에서는 다양한 유형의 컨트롤러에 대한 쉘 뫼르딕 CAST 분석의 예를 보여준다. 프로세스 컨트롤 시스템 분석에서는 자동화된 컨트롤러의 예시를 제공한다. 쉘 뫼르딕 화학 플랜트의 또 다른 컨트롤러는 사람 또는 그룹이었다. 공간상의 이유로 여기에서도 세부 사항은 생략되었다.

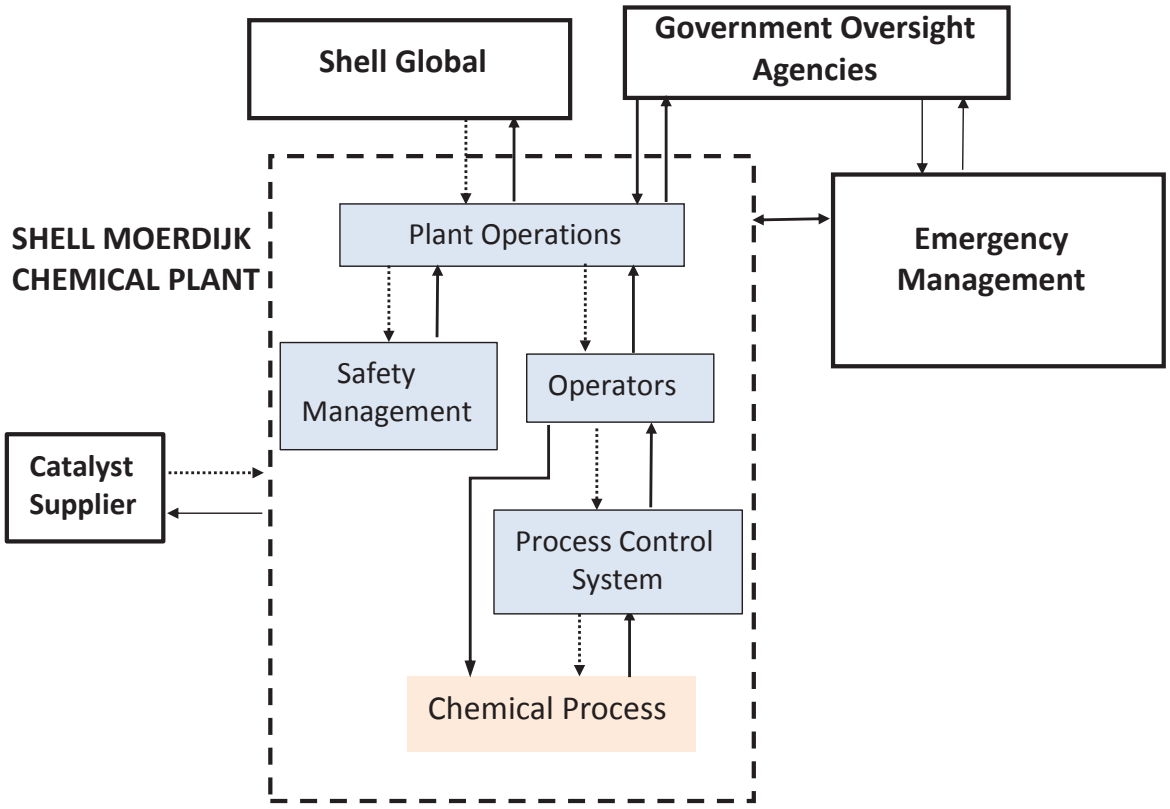



**Figure 15**: Shell Moerdijk Chemical Plant Safety Control Structure.

## Operators

The operators' actions clearly contributed to the explosions. For example, they manually added additional warmth to the ethylbenzene at a time when heat was increasing precipitously; they did not notice and respond to hot spots and negative pressure differential; they did not respond appropriately to alarms; they left the gas discharge system closed when the gas was increasing; they did not stabilize, slow down, and stop the process when pre-set limits were exceeded (which is a fundamental principle in operator training at Shell); etc.

Given all these things that in hindsight the operators did wrong, they appear to have major responsibility for the loss. In fact, listing these actions is where many (most?) accident causal analyses and accident reports stop and the operators are deemed to be the major cause of the loss. While it is possible that everyone working the turnaround that day was negligent and irresponsible, it is more likely that they were trying to do their best. Without understanding *why* they made bad decisions, i.e. why the decisions seemed correct to them at the time, we cannot do much about preventing similar flawed decision making in the future. Many of the answers lie in higher levels of the control structure, but some of the operators' actions can be understood by looking at their process models and the context in which they were making decisions.

The relevant general safety-responsibilities assigned to the operators:

- Operate the plan in a way that does not lead to hazards
  - Monitor plant conditions and alarms
  - Control the process such that it stays within safe boundaries of operation
  - Respond to unsafe conditions that occur

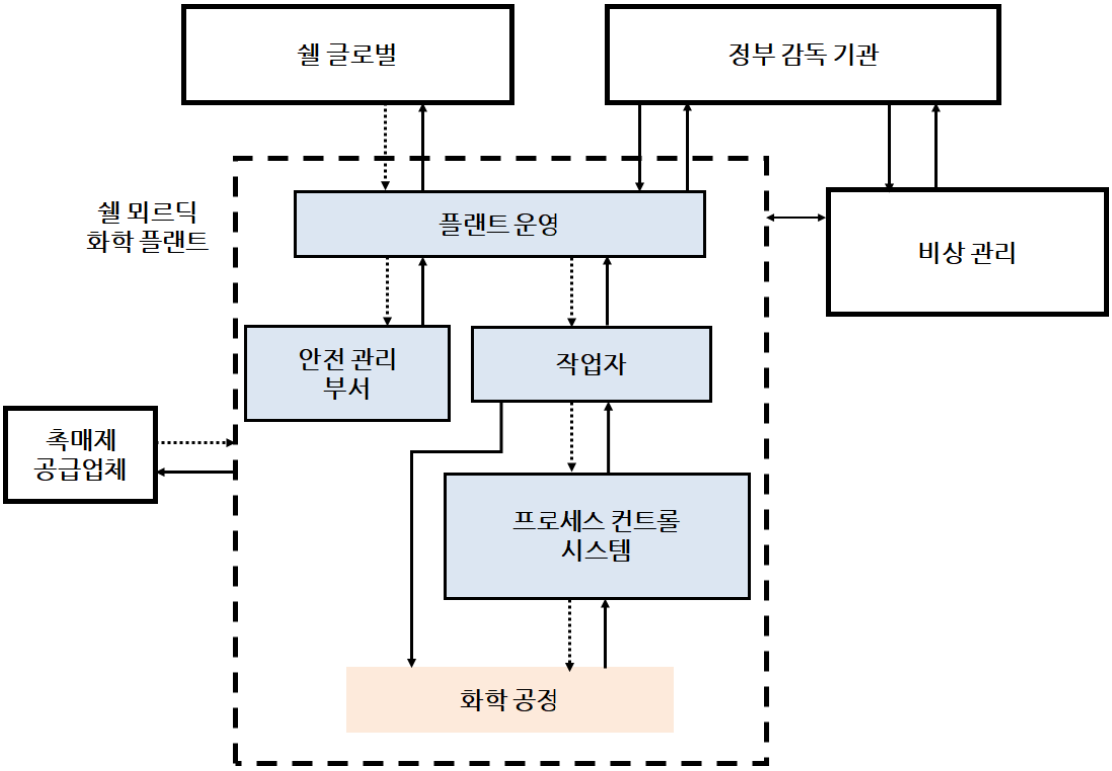



그림 15: 쉘 뫼르딕 화학 플랜트의 안전 컨트롤 스트럭처

### 운영자(Operators)

운영자의 행동은 분명히 폭발에 기여했다. 예를 들어, 그들은 열이 급격하게 증가하고 있는 시점에서 수동으로 에틸벤젠에 추가적인 열을 가했다; 그들은 핫 스팟과 음압(negative pressure)의 차이를 알아차리지 못했고 대응하지 않았다; 그들은 경보에 대해 적절하게 대응하지 않았다; 그들은 가스가 증가하고 있을 때 가스 배출 시스템을 닫아 두었다; 그들은 사전에 설정된 한계점을 초과했을 때 안정시키거나 감속하지 않았고 프로세스를 중단(쉘의 운영자 훈련 기본 원칙)하지 않았다; 등이 있다.

이러한 모든 것들을 사후에 고려해보면 운영자들이 손실에 대해 중대한 책임을 가진 것처럼 보인다. 실제로 이러한 행동들을 나열하는 것은 많은(대부분?) 사고 원인 분석 및 사고 보고를 중단시키고 운영자를 손실의 주요 원인으로 간주하는 결과를 낳게 된다. 그 날, 턴어라운드 작업을 하는 모든 사람들이 태만하고 무책임했을 가능성도 있지만 최선을 다하려고 노력했을 가능성이 더 크다. 그들이 *왜* 잘못된 결정을 내렸는지 이해하지 못한다면, 즉, 그 당시에 그 결정들이 그들에게 왜 옳은 것처럼 보였는지 이해하지 못한다면, 향후 유사한 잘못된 의사결정을 방지하기 위해 우리가 할 수 있는 것은 많지 않다. 많은 답이 컨트롤 스트럭처의 상위 수준에 존재하겠지만 운영자의 행동 중 일부는 프로세스 모델 및 그들이 의사결정을 했던 상황(context)을 살펴봄으로써 이해할 수 있다.

운영자에게 할당된 일반적인 안전 책임:

- 위험을 유발하지 않는 방식으로 플랜트를 운영한다.
  - 플랜트의 상태와 경보를 모니터링 한다.
  - 안전한 작동 범위 내에서 동작하도록 프로세스를 컨트롤한다.
  - 발생한 안전하지 않은 조건에 대응한다.

| |
|---|
| And specific to this incident:<br>• Adjust gas and liquid flows as needed during startup<br>• Make sure the Unit is not heated too quickly (in part to prevent damage to the catalyst pellets) |

None of these responsibilities were fulfilled. Examples of operator behavior that contributed to the hazardous state include:

- The operators did not stabilize or halt process before the explosion when critical process boundaries were exceeded.
- Heating was started (around 21:00) while the situation was still unstable and after only 45 minutes of wetting. Proper wetting had probably not been achieved by that time.
- The operators manually added additional warmth to the ethylbenzene at a time when heat was increasing precipitously.
- The operators did not notice and respond to hot spots. They also did not notice and respond to the related negative pressure differential.
- The operators did not properly adjust nitrogen flow. The lower (than required) nitrogen flow was one of the causes of the accident.
- The operators did not respond to alarms.

Looking only at these behaviors, the behavior of the operators seems egregious. This is where most accident reports stop. But the picture looks very different when the contextual factors and process model flaws are considered. Because of space reasons, only a few examples of these are provided below. The reader is referred to the full analysis in the CAST report for the more detailed analysis.

| Why? (Contextual Factors Affecting the Unsafe Control) | Questions Raised |
|---|---|
| The operators were not provided with the information they needed to make correct decisions. The process control system provided almost no support (feedback). Throughout the accident report, there are many actions by the operator that are noted to require intense attention and deep understanding of the process dynamics. | *Why? Was any human factors analysis done when the decision was made to have the operators manually control startup to ensure that they were capable of doing this reliably? And without process control system support?* |
| Adjusting gas and liquid flows was known to be difficult, partly because of weaknesses in the design of the central pump. In addition, the job analysis does not provide clear instructions about how the filling and circulation has to be done. The only clear instruction was that the central pump not be allowed to run “dry” or it would break. | |
| Safety during the heating and wetting of the reactors was dependent on the knowledge and skill of the operators and production team leader on duty at the time. Shell Moerdijk’s written policies required that the starting and stopping of the reactors had to be done by experienced operators using the work instructions provided for this purpose. However, while the personnel performing this maintenance stop were experienced staff and were trained for working on this unit | |

그리고 이 사건에 대한 구체적인 책임:

- 기동 중에 필요에 따라 가스와 액체 유량을 조정한다.
- Unit이 너무 빨리 가열되지 않도록 한다(촉매제 펠릿의 손상 방지를 위한 측면에서).

위의 책임 중 어느 것도 이행되지 않았다. 위험한 상태에 기여한 운영자 행동의 예는 다음과 같다:

- 크리티컬한 프로세스 경계를 넘어섰을 때 운영자가 폭발 전에 프로세스를 안정시키거나 중단하지 않았다.
- 상황이 여전히 불안정한 상태에서 단지 45분만의 습윤(wetting) 후에 가열이 시작되었다(약 21:00경). 그 시간까지 적절한 습윤이 이루어지지 않았을 것이다.
- 열이 급격히 증가하는 시점에 수동으로 에틸벤젠에 추가 열을 가했다.
- 운영자들은 핫스팟을 알아채지 못하고 대응하지 않았다. 또한 관련 음압 차이에 대해서도 알아차리지 못하고 대응하지 않았다.
- 운영자들이 질소 유량을 제대로 조정하지 못했다. (요구되는 것보다) 낮은 질소 유량은 사고의 원인 중 하나였다.
- 운영자들이 경보에 대응하지 않았다.

이런 행동들만 보면 운영자의 행동은 매우 나쁘게 보인다. 대부분의 사고 보고가 중단되는 지점이 바로 이 지점이다. 그러나 컨텍스트적 요인과 프로세스 모델의 결함을 고려하면 상황은 매우 다르게 보인다. 공간상의 이유로 아래 몇 가지 예시만 제시한다. 보다 자세한 분석은 CAST 보고서의 전체 분석을 참조하도록 한다.

| **왜? (안전하지 않은 컨트롤에 영향을 미치는 컨텍스트적 요인)** | **제기된 질문** |
|---|---|
| 운영자는 올바른 결정을 내리는 데 필요한 정보를 제공받지 못했다. 프로세스 컨트롤 시스템은 지원(피드백)을 거의 제공하지 않았다. 사고 보고서 전체에 걸쳐, 프로세스 변동성에 대한 집중적 주의와 깊은 이해가 필요하다고 언급된, 운영자가 수행해야 할 행동이 많이 있었다. | *왜? 운영자가 기동을 수동으로 제어하며 이를 안정적으로 수행할 수 있다고 결정했을 때 인적요인 분석이 수행되었는가? 그리고 프로세스 컨트롤 시스템의 지원이 없어도 되는가?* |
| 중앙 펌프 설계의 취약점으로 인해 가스 및 액체 유량 조정은 어려운 것으로 알려져 있었다. 또한 직무 분석에서 충전 및 순환을 수행하는 방법에 대한 명확한 지침을 제공하지 않았다. 유일하게 명확한 지침은 중앙 펌프가 “건조한” 상태로 가동되지 않아야 한다는 것이고 그렇지 않으면 고장난다는 것이었다. | |
| 반응로의 가열 및 습윤 과정에서의 안전은 당시 운영자와 생산팀 리더의 지식 및 기술에 달려있었다. 쉘 뫼르딕의 서면 정책에는 반응로의 시작과 정지는 숙련된 운영자가 작업 지침을 사용하여 수행해야 한다고 되어 있었다. 그러나 유지보수를 위해 운영 중단을 수행하는 직원은 정상적인 생산 단계에서는 경험이 풍부했고 훈련을 받았지만, 촉매제 교체는 3~4년에 한 | |

| | |
|---|---|
| during regular production, a catalyst change only occurs once every three or four years and this was their first experience with restarting the reactor. At the same time, they were not provided with support from the process control system for this startup. | |
| The accident report says that the start-up procedures had been followed correctly by the operators. The problem, then, must have been in the procedures themselves. In fact, the work instructions used by the operators were incorrect and incomplete. The work instructions did not follow the format provided by Shell for such instructions and omitted much of the required information such as critical conditions and required steps to be taken by the operators. Nitrogen flow was not considered critical, for example, and was not included in the work instructions although it turned out to be critical after the fact. | *Why were incorrect and incomplete work instructions provided to the operators?* |
| The startup procedures were produced by the operators. There does not seem to have been any expert review by engineers and safety personnel. The accident report provides no explanation for *w*hy operators are writing their own work instructions for safety-critical operations without at least expert review by engineers and safety personnel. | *The report does not answer the obvious questions here: Were the work instructions produced by the operators performing the startup (who had no experience)? If it was other operators, did they have the experience and knowledge to create the work instructions? Who reviews these work instructions? Were they reviewed by anyone? (The answer to this question appears to be no).* |
| There is a design book, created by Shell Global Projects and Technology, that contains detailed information about the design and operation of the reactor. The Design Book was not used in creating the work instructions for the startup because, the accident report says, the book was too detailed and "intricately presented" and was not understandable by the operators charged with drawing up the work instructions. | *There are many obvious questions raised here.* |

| Why? (Process Model Flaws) | Questions Raised |
|---|---|
| There was a lot of hindsight bias in the accident report describing what the operators "should have" done, but the conditions that occurred were all consistent with their expectations (process model) given the conditions during previous maintenance stops. The operators considered fluctuations in pressure to be normal during restarts (process model flaw). The pressure had fluctuated continually since the beginning of the restart. Such | *Why were the expectations (their mental models of process behavior) not correct in this instance?* |

| 왜? (안전하지 않은 컨트롤에 영향을 미치는 컨텍스트적 요인) | 제기된 질문 |
|---|---|
| 번만 이루어지므로 이번 반응로 재가동은 그 직원에게는 첫 번째 경험이었다. 동시에 그들은 이 기동을 위한 프로세스 컨트롤 시스템의 지원을 제공받지 못했다. | |
| 사고 보고서에 따르면 기동 절차를 운영자가 올바르게 수행했다고 한다. 그렇다면 문제는 그 절차 자체에 있었던 것이 틀림없다. 실제로 운영자들이 사용하는 작업 지침은 정확하지 않았고 불완전했다. 작업 지침은 쉘이 제공한 형식을 따르지 않았으며 중요한 조건 및 운영자가 취해야 할 필수 단계와 같은 필요 정보가 상당 부분 생략되었다. 예를 들어 사후에 중요한 것으로 밝혀진 질소 유량은 중요하게 고려되지 않았으며 작업 지침에도 포함되지 않았다. | *운영자에게 부정확하고 불완전한 작업 지침이 제공된 이유는 무엇인가?* |
| 기동 절차는 운영자에 의해 만들어졌다. 절차에 대한 엔지니어 및 안전 담당자에 의한 전문가 검토는 없었던 것으로 보인다. 사고 보고서에는 운영자가 안전-중요 작업에 대한 엔지니어 및 안전 담당자의 최소한의 전문가 검토 없이 자신들의 작업 지침을 작성하고 있었던 이유를 설명하지 않았다. | 그 보고서는 여기서 명백한 질문에 대해 답변하지 않는다. 기동을 수행하는 운영자(경험이 없는 사람)가 작성한 작업 지침이 있는가? 만약 다른 운영자가 작성하였다면, 그는 업무 지침을 작성할 수 있는 경험과 지식을 가지고 있었는가? 누가 이런 작업 지침을 검토하는가? 그 작업 지침을 누구라도 검토하였는가?(이 질문에 대한 답은 아니오인 것 같다.) |
| 쉘 글로벌 프로젝트 앤 테크놀로지(Shell Global Projects and Technology)가 만든 설계서가 있는데, 이 설계서에는 반응로의 설계와 운영에 대한 상세한 정보가 있다. 사고 보고서에 따르면 그 책은 너무 상세하고 “복잡하게 표현되었다”라고 하고 있으며, 작업 지침을 작성하는 운영자들이 이해할 수 없었다. 그래서 기동에 대한 작업 지침을 만드는 데 사용되지 않았다. | 여기서 제기되는 명백한 질문들이 많이 있다. |

| 왜? (프로세스 모델 결함) | 제기된 질문 |
|---|---|
| 운영자가 “했어야 하는” 것을 설명하는 사고 보고서에는 사후확신 편향이 많이 있었지만, 이전의 유지보수 중지 기간 동안의 조건을 고려하였을 때 발생한 조건은 모두 그들의 기대(프로세스 모델)와 일치했다. 운영자들은 재구동 과정에서 압력이 오르내리는 것을 정상으로 간주했다(프로세스 모델 결함). 재구동이 시작된 후부터 압력은 계속 변동하였다. 이러한 변동은 이전 재구동 과정에서도 발생해왔었고 따라서 그들이 예상했던 것이었다. 물론 사후에는 이러한 예상이 잘못된 것으로 판 | 이 예시에서 왜 예상(프로세스 동작에 대한 그들의 멘탈 모델)이 맞지 않았는가? |

| | |
|---|---|
| fluctuations had occurred during previous restarts and that was what they expected. In hindsight, of course, these expectations turned out to be wrong. Given the situation, the number of alarms that sounded and their frequency was not out of the ordinary, without knowing *after the fact* that the process was indeed not in an ordinary state. | |
| The accident report says that the ability to make an assessment to intervene in special situations requires knowledge of, experience with, and thorough preparation for such special situations. The operators must fully grasp what caused the unit to exceed limits in order to assess risk. The operator did not have the required knowledge or expertise.<br>. In fact, even the corporate safety engineers did not know that the conditions that occurred here could result in a hazardous state. If the designers did not believe such scenarios were possible, why would the operators? In fact, nobody at Shell thought that a scenario involving a fast and high-pressure buildup was possible. | *Why did the designers and corporate safety engineers believe that such scenarios were impossible?* |

In summary, the actions of the operators look much less clearly negligent when the reasons why the operators behaved the way they did is the focus of the investigation rather than a focus on what the operators did that turned out to be wrong. The operators, in fact, acted appropriately or at least understandably given the context, the incorrect work instructions (which they followed), and their lack of training and required skill and knowledge in performing the work. In addition, they were provided with almost no assistance from the process control system. As many of the tasks they needed to do required intense attention, precision, mental effort, deep understanding of process dynamics, and frequent adjustments to a continually fluctuating process, such assistance would have been invaluable.

The designers of the plant did not recognize or understand the risks (see the appropriate sections of the CAST analysis) so the risks might not have been communicated thoroughly to the operators. Management seemed to rely on operators seeing something strange and stopping the process, but did not provide the information and training to ensure it was possible for operators to do this. Such a policy provides a convenient excuse to blame the operators after an accident, but it does not help the operators to carry out their responsibilities.

Generating recommendations will be covered later, but some obvious ones from this part of the analysis are that the operators must have the appropriate skills and expertise to perform their assigned activities, and there must be someone overseeing operations who is assigned the responsibility for implementing this requirement. Other possible recommendations include the need for a human factors study during the job analysis to ensure that the operators are provided with information and a work situation that allows them to make appropriate decisions under stressful conditions, better automated assistance during all phases of operation, training for activities that are known to be hazardous such as startup, and finally improved work instructions together with a better process for producing them.

This analysis, as usual, raises a lot of additional questions that need to be answered in order to understand what happened and make recommendations to prevent such occurrences in the future. These will be summarized in the rest of the section of the handbook (with the details omitted) so that readers have a fuller picture of the CAST process and the results that can be obtained from it.

| 왜? (프로세스 모델 결함) | 제기된 질문 |
|---|---|
| 명되었다. 프로세스가 정말 정상 상태가 아니었다는 사실을 그 때 알지 못했다 하더라도, 주어진 상황에서 울렸던 경보음의 수와 그 빈도는 정상이 아니었다. | |
| 사고 보고서에 따르면 특수한 상황에 개입하기 위한 평가를 수행하려면 이러한 특수 상황에 대한 지식, 경험 및 철저한 준비가 필요하다. 리스크를 평가하기 위해서 운영자는 유닛이 한계를 초과한 원인이 무엇인지 완전하게 파악해야 한다. 운영자는 필요 지식이나 전문지식이 없었다. 실제로 기업의 안전 엔지니어들조차 여기서 발생한 조건이 위험한 상태를 초래할 수 있다는 것을 알지 못했다. 만약 설계자들이 이런 시나리오가 불가능하다고 믿었다면 왜 운영자들이 그런 시나리오가 가능하다고 믿겠는가? 실제로 쉘의 어느 누구도 급격한 고압상황을 유발하는 시나리오를 가능하다고 생각하지 않았다. | 설계자와 기업의 안전 엔지니어들은 왜 그러한 시나리오가 불가능하다고 믿었는가? |

요약하자면, 운영자들의 잘못된 행동을 판단하는 것에 초점을 맞추기보다는 조사에 초점을 맞췄을 때 운영자들이 분명히 훨씬 덜 부주의한 것으로 보인다. 실제로, 당시의 상황(컨텍스트), (그들이 따랐던) 잘못된 작업 지침, 업무 수행에 필요한 훈련, 기술 및 지식의 부족을 고려한다면; 운영자들은 적절하게 또는 적어도 이해할 수준으로 행동한 것이다. 또한 그들은 프로세스 컨트롤 시스템의 지원을 거의 받지 못했다. 그들이 해야 하는 많은 업무는 높은 주의력, 정밀함, 정신적 노력, 프로세스 변동성에 대한 깊은 이해, 그리고 지속적으로 변동하는 프로세스에 대한 잦은 조정을 필요로 했기 때문에 그러한 지원은 매우 중요했을 것이다.

플랜트 설계자가 리스크를 인지 또는 이해하지 못했기 때문에(CAST 분석의 해당 섹션 참조) 운영자에게 리스크가 완전히 전달되지 않았을 수도 있다. 관리자는 운영자가 이상한 상황을 알아차리고 프로세스를 중단하는 것에 의존하는 것처럼 보였지만 운영자가 이러한 것을 수행할 수 있도록 하는 정보와 교육을 제공하지는 않았다. 이러한 방침은 사고 후 운영자를 비난할 수 있는 편리한 변명이 되지만 운영자가 그들의 책임을 수행하는 데에는 도움이 되지 않는다.

권고사항을 만드는 것은 나중에 다루겠지만 분석의 이 부분에서 몇 가지 분명한 권고사항은, 운영자들은 할당된 업무를 수행하기 위해 적절한 기술 및 전문 지식을 갖추어야 하고, 이 요구사항을 이행할 책임을 부여받은, 작업을 감독하는 누군가가 있어야 한다는 것이다. 다른 가능한 권고사항으로는, 스트레스가 많은 조건에서도 운영자가 적절한 결정을 내릴 수 있게끔 운영자가 정보 및 작업 상황을 제공받도록 보장하는 업무 분석에서의 인적 요인에 대한 연구, 모든 작업 단계에서의 더 나은 자동화된 지원, 기동과 같이 위험하다고 알려진 작업에 대한 훈련, 그리고 마지막으로 업무 지침 및 업무 지침 생성 프로세스 개선에 대한 필요성을 포함할 수 있다.

늘 그렇듯이 이러한 분석은 답변해야 하는 추가 질문을 많이 제기하게 하는데 이는 무슨 일이 있었는지 이해하고 향후 그러한 일이 발생하지 않도록 권고하기 위함이다. 이 내용은 핸드북의 나머지 섹션에 요약했으며 독자들은 CAST 프로세스와 그 결과에 대한 완전한 그림을 볼 수 있을 것이다.

So far, we have looked at the physical process, the automated process control system, and the plant operators. We now briefly look at the role that the CAST analysis identifies that each of the other controllers played in the loss, working our way up the safety control structure. Once again, detailed CAST analyses for each controller is not included in this handbook but can be found elsewhere.

## Plant Safety Management

The plant safety department usually provides oversight of operational safety and provides information to plant operations management to ensure that operational decisions are made with safety in mind. Examples of the detailed analyses are included here, but we have found that too much detail discourages reading of the report. A useful compromise is to include the detail but also include a summary of the role in the component in the accident that summarizes the important points of the detailed analysis.

Relevant Responsibilities of Plant Safety Management

- Identify plant hazards and ensure that they are eliminated, mitigated, or controlled.
- Either provide work instructions for safety-critical activities or review the work instructions provided by someone else for their safety implications.
- Ensure appropriately trained, skilled, and experienced people are assigned to high risk processes.
- Follow the Management of Change (MOC) procedures by doing a risk assessment for changes and implement risk controls based on the results.
- Provide for emergency treatment to exposed or injured individuals and ensure required medical equipment and personnel is available at all times. [*The injured personnel were treated effectively on the scene so this aspect is not considered further.*]
- Perform audits of safety-critical activities or assist plant operations management in performing such audits [*It is not clear from the accident report who is responsible for audits but there do appear to have been audits.*]

Process Model Flaws of the plant safety managers

- Regarded ethylbenzene as a safe substance in this process.
- Considered the start-up process not to be high risk.
- Thought that the Operators and the Production Team Leader could manage and control the start-up manually based on their knowledge and experience.
- There were so sure that they understood the risks that even incidents at other similar plants did not trigger any doubts about their assumptions. Alternatively, they may not have been made aware of the previous incidents.

A Few Example Contextual/Process Model Factors (more included in summary below):

- Over time, understanding of the most appropriate procedures relating to Unit 4800 changed. Some of the procedures were not considered critical to safety. So, these procedures were not included (or were no longer included) in the amended work instructions.
- Safety assessment procedures complied with government requirements.
- Hazard assessment focused on processes that were considered higher risk and primarily assessed the effects of substances on the environment and not on safety.

지금까지 물리적 프로세스, 자동화된 프로세스 컨트롤 시스템, 그리고 플랜트 운영자에 대해 살펴봤다. 이제 CAST 분석에서 식별한 손실에서의 각 컨트롤러의 역할을 간략히 살펴보고 안전 컨트롤 스트럭처를 개선할 것이다. 다시 말하지만, 이 핸드북에 각 컨트롤러에 대한 상세한 CAST 분석은 포함되어 있지 않지만 다른 곳에서 별도로 확인할 수 있다.

### 플랜트 안전 관리 부서(Plant Safety Management)

플랜트 안전 부서는 일반적으로 운영 안전에 대한 감독을 수행하고, 플랜트 운영 관리에 정보를 제공하여 안전을 염두에 두고 운영 결정이 이루어지도록 한다. 아래에 상세 분석의 예시가 있지만 너무 자세한 내용은 오히려 보고서를 읽는데 방해가 되므로 절충안으로, 상세 내용을 포함시키되 중요한 점을 요약하여 사고에서의 컴포넌트 역할 요약과 함께 기술한다.

플랜트 안전 관리 부서의 관련 책임

- 플랜트의 위험을 식별하고, 제거, 완화 또는 통제되는지 확인한다.
- 안전-중요 활동에 대한 작업 지침을 제공하거나 다른 사람이 제공한 작업 지침이 안전에 미치는 영향을 검토한다.
- 충분히 훈련되고 숙련되며 경험이 풍부한 사람을 리스크가 높은 프로세스에 배정한다.
- 변경사항에 대한 리스크 평가를 수행함으로써 변경관리(MOC) 절차를 준수하고 리스크 평가 결과에 따라 리스크 컨트롤을 수행한다.
- 유해 환경에 노출되거나 부상당한 사람에게 응급 치료를 제공하고 필요한 의료 장비와 인력이 항상 가용하도록 한다. [*부상자는 현장에서 효과적으로 치료되었으므로 이 측면은 더 이상 고려되지 않는다.*]
- 안전-중요 활동을 감사하거나 그러한 감사를 수행할 때 플랜트 운영 관리를 지원한다. [*사고 보고서에서 누가 감사를 책임지는지는 분명하지 않지만 감사가 수행된 것으로 보인다.*]

플랜트 안전 관리자의 프로세스 모델 결함

- 이 프로세스에서 에틸벤젠을 안전한 물질로 간주했다.
- 기동 프로세스의 리스크가 높지 않다고 간주했다.
- 운영자와 생산팀 리더는 지식과 경험을 바탕으로 기동을 수동으로 관리하고 컨트롤할 수 있다고 생각했다.
- 그들이 리스크를 이해한다는 확신이 너무 강해서 다른 유사 플랜트에서 일어난 사건조차도 가정에 대한 의심을 불러일으키지 못했다. 또는 이전 사건들을 알지 못했을 수도 있다.

컨텍스트적/프로세스 모델 요소의 몇 가지 예제(아래 요약에 더 포함됨):

- 시간이 흐르면서 Unit 4800의 가장 적절한 절차에 대한 이해가 바뀌었다. 일부 절차는 안전에 중요하지 않다고 간주되었다, 따라서 이러한 절차는 수정된 작업 지침에 포함되지 않았다(또는 더 이상 포함되지 않았다).
- 안전 평가 절차는 정부의 요구사항을 준수했다.
- 위험 평가는 리스크가 높다고 간주되는 프로세스에 초점을 맞추었고 주로 안전이 아닌 환경에 영향을 미치는 물질을 평가했다.

Summary of the Role that Shell Moerdijk Safety Management Played in the Accident:

- The safety analysis methods used were either not appropriate, not applied or were applied incorrectly. However, the methods used complied with the Shell requirements and satisfied the Dutch legal and regulatory requirements. They were also standard in the petrochemical industry. Safety management did not consider certain relevant information nor investigate how ethylbenzene reacting with the catalyst could cause an explosion. Safety management at Shell Moerdijk, as is common in many places, seems to have been largely ineffectual, with lots of activity, but much of it directed to minimal compliance with government regulation. A partial explanation for their behavior is that everyone believed that a reaction between ethylbenzene and the catalyst was impossible and that the start-up process was low risk.
- Although Shell's safety management system includes requirements for dealing with changes, the Management of Change (MOC) procedures were not followed nor implemented effectively. Risks resulting from changes made to the plant, the catalyst, the processes, and the procedures were not identified and managed. Not following MOC procedures has been implicated in a very large number of accidents in all industries.
- A new catalyst was selected for use at Shell Moerdijk, but an assumption was made that the properties of the new catalyst were the same as those of the previous catalyst. The altered composition of the new catalyst was stated in the safety information sheet provided by the manufacturer, but safety engineering did not notice this change.
- Procedure changes (heating rate and nitrogen flow) were instituted without a risk assessment. These procedures were not included in the amended operator work instructions. Other plant and production changes were not systematically examined for their safety effects on the basis of a risk analysis in all cases. Only a few failure scenarios were examined, but this fulfilled both Shell Global and Dutch law. There were never any safety studies that focused on the circulation and heating of the unit involved in the accident. Safety was based on studies done in 1977 that had shown the catalyst (as it then existed) was inert in the presence of ethylbenzene. This assumption was never reassessed even though the composition of the catalyst changed over time and similar incidents occurred at other Shell installations. There were no requirements by either Shell Global or the Netherlands law to do so.
- The number of leaks was used as the primary leading indicator of process safety, which clearly has nothing to do with this accident. Because the number of leaks had been greatly reduced in recent years, decision makers assumed safety was improving. The use of this leading indicator is common in the petrochemical industry and was accepted by the Dutch regulatory authorities.
- Similar incidents occurred at Shell Nanhai and at Shell Moerdijk after initial startup in 1999. No explosion occurred at Nanhai because of special factors. These events did not trigger a response in terms of reassessing risk or procedures or the assumptions that a runaway was impossible. Recommendations following the Nanhai incident were not used to reduce risk. *Why? There is no information in the accident report about why the Nanhai incident recommendations were not implemented.*
- Safety engineering did not provide proper oversight of the generation of work instruction, which allowed unsafe work instructions to be provided to the operators. The work instructions did not follow the format provided by Shell for such instructions. They also omitted much of the required information such as critical conditions and required steps to be taken by the operators.

쉘 뫼르딕 안전 관리가 사고에서 수행한 역할 요약:

- 사용된 안전 분석 방법이 적절하지 않았거나, 적용되지 않았거나 또는 잘못 적용되었다. 그러나 사용된 방법은 쉘 요구사항을 준수하고 네덜란드의 법률 및 규제 요구사항을 충족시켰다. 또한 그 방법은 석유 화학 산업계에서의 표준이었다. 안전 관리 부서는 특정한 유관 정보를 고려하지 않았고 에틸벤젠이 어떻게 촉매제와 반응하여 폭발을 일으킬 수 있는지도 조사하지 않았다. 다른 많은 곳과 마찬가지로 쉘 뫼르딕의 안전 관리 부서의 많은 활동은 대체로 효과가 없는 것처럼 보였지만 그 중 대부분은 최소한 정부 규제를 준수하고 있었다. 그들의 행동에 대한 일부 설명에서는 모든 사람들이 에틸벤젠과 촉매제 사이의 반응은 불가능하며 기동 프로세스의 리스크는 낮은 것으로 믿었다고 한다.
- 쉘의 안전 관리 시스템은 변경사항을 처리하기 위한 요구사항을 포함하고 있지만 변경관리(MOC) 절차는 준수되지도 효과적으로 시행되지도 않았다. 플랜트, 촉매제, 프로세스 및 절차의 변경으로 인한 리스크는 식별되거나 관리되지 않았다. 변경관리 절차를 따르지 않는 것은 모든 산업에서의 매우 많은 사고와 관련이 있다.
- 쉘 뫼르딕에서 사용할 새로운 촉매제를 선택했지만 새로운 촉매제의 특성이 이전 촉매제의 특성과 동일하다는 가정이 있었다. 새로운 촉매제의 변경된 구성은 제조업체가 제공한 안전 정보 시트에 명시되어 있었지만 안전 엔지니어링에서는 이러한 변경사항을 알아차리지 못했다.
- 리스크 평가 없이 절차 변경(가열율 및 질소 유량)을 시행했다. 이러한 절차는 운영자의 수정된 작업 지침에 포함되지 않았다. 다른 플랜트와 생산의 모든 변경사항에 대해 리스크 분석에 기반한 안전 영향이 체계적으로 검사되지 않았으며, 단지 몇 개의 실패 시나리오만 검토되었는데도 쉘 글로벌 및 네덜란드 법률을 모두 충족시켰다. 사고에 관련된 유닛의 순환 및 가열에 초점을 맞춘 안전 연구는 전혀 없었다. 안전은 1977년에 행해진 연구에 기초하였는데 이 연구는 (당시 존재했던) 촉매제가 에틸벤젠의 존재 하에서 불활성임을 보여주었다. 시간이 지남에 따라 촉매제의 구성이 바뀌었고 다른 쉘 설비에서 유사한 사건이 발생했음에도 불구하고 이 가정은 결코 재평가되지 않았다. 쉘 글로벌이나 네덜란드 법률에도 재평가해야 한다는 요구사항은 없었다.
- 누출 횟수는 공정 안전의 주요 선행지표로 사용되었으며 이는 이 사고와는 아무런 관련이 없다. 최근 몇 년 동안 누출 횟수가 크게 줄었기 때문에 의사결정권자는 안전이 개선되고 있다고 여겼다. 이 주요 선행지표의 사용은 석유 화학 산업에서는 일반적이며 네덜란드 규제 당국에 의해 수용되었다.
- 1999년 초기 스타트업 이후 쉘 난하이와 쉘 뫼르딕에서도 유사한 사건이 발생하였다. 난하이에서는 특수한 요인으로 인해 폭발이 발생하지 않았다. 이러한 이벤트를 경험한 후에도 리스크나 절차의 재평가 또는 폭주가 불가능하다는 가정에 대한 개선이 이루어지지 않았다. 난하이 사건에 따른 권고사항은 리스크를 줄이기 위해 사용되지 않았다. *왜? 사고 보고서에는 난하이 사건의 권고사항이 시행되지 않은 이유에 대한 정보가 없었다.*
- 안전 엔지니어링은 작업 지침 생성에 대한 적절한 감독을 제공하지 않았고 안전하지 않은 작업 지침을 운영자에게 제공하게 하였다. 작업 지침은 쉘이 제공한 형식을 따르지 않았다. 또한 중요한 조건 및 운영자가 취해야 할 필수 단계와 같은 필요한 정보의 상당 부분이 누락되었다.

Recommendations:

While the problems specific to the explosions on 3 June 2014 should be fixed, there were a lot of weaknesses in the Shell Moerdijk safety management practices identified in the official Dutch Safety Agency accident report and in the CAST analysis. These need to be improved.

- Safety management at Shell Moerdijk needs to be made more effective. Safety engineering needs to be more than just going through the motions and minimally complying with standards.
- All work instructions should be reviewed for safety by knowledgeable people using information from the hazard analysis. [In this case, the hazard analysis was flawed too, but that is a different problem to fix.]
- MOC procedures must be enforced and followed. When changes occur, assumptions of the past need to be re-evaluated.
- Hazard analysis and risk assessment methods need to be improved.
- More inclusive and relevant leading indicators of risk need to be established.
- Procedures for incorporating and using lessons learned need to be established or improved.

## Operations Management

Relevant Safety-Related Responsibilities

- Establish safety policy for operations.
- Ensure that Safety Management is fulfilling their responsibilities and providing realistic risk and hazard assessments.
- Use the results of the hazard and risk analyses provided by Safety Management in decision making about plant operations.
- Create a Shell Moerdijk Safety Management System consistent with the overall Shell Global Safety Management System, ensuring it is both effective and being followed.

More specific safety-related responsibilities include the following:

- Provide appropriate training for operators for nominal and off-nominal work activities.
- Follow MOC (Management of Change] procedures that require performing a risk assessment for changes or ensure that safety management is doing so. Use the risk assessment to provide oversight of the process and to design and implement risk controls in the plant and the operating procedures.
- Prepare (or at least review) the work instructions. Ensure they are safe and are being followed.
- Minimize the number of personnel in the vicinity (at risk) during high-risk operations, such as during a turnaround.
- Keep records of incidents and lessons learned and ensure they are communicated and used by those that need to learn from them.
- Provide personnel assignments that are commensurate with the experience and training required for the activity.
- Provide a process control system that can assist operators in performing critical activities.
- Conduct audits. Establish leading indicators to be used in the audits (and in other feedback sources) or ensure that safety engineering is identifying appropriate leading indicators.

권고사항 :

2014년 6월 3일에 발생한 폭발 문제가 해결되어야 하는데, 네덜란드 안전청의 공식적인 사고 보고서와 CAST 분석에서 확인된 쉘 뫼르딕의 안전 관리 관행에는 많은 취약점이 있었다. 이러한 것들이 개선될 필요가 있다.

- 쉘 뫼르딕의 안전 관리를 보다 효과적으로 개선할 필요가 있다. 안전 엔지니어링은 단순히 형식적으로 수행하는 것 그리고 최소 수준으로 표준을 준수하는 것 이상이 필요하다.
- 모든 작업 지침은 지식이 풍부한 사람이 위험 분석 관련 정보를 활용하여 안전 측면에서 검토해야 한다. [이 사건의 경우 위험 분석에도 결함이 있었는데 그것은 개선되어야 할 또 다른 문제이다.]
- 변경절차가 시행되고 지켜져야 한다. 변경사항이 있는 경우 기존의 가정을 재평가해야 한다.
- 위험 분석 및 리스크 평가 방법을 개선해야 한다.
- 더 나은 리스크 선행지표를 식별하고 사용해야 한다.
- 교훈을 반영하고 사용하는 절차를 수립하거나 개선해야 한다.

## 운영 관리(Operation Management)

안전 관련 책임

- 작업을 위한 안전 정책을 수립한다.
- 안전 관리 조직이 책임을 이행하고 현실적인 리스크 및 위험 평가를 제공하도록 한다.
- 안전 관리 조직에서 제공하는 위험 및 리스크 분석 결과를 플랜트 운영에 대한 의사결정에 활용한다.
- 쉘 글로벌 안전 관리 시스템과 동일한 쉘 뫼르딕 안전 관리 시스템을 구축하여 효과적으로 운영하고 따르도록 한다.

보다 구체적인 안전 관련 책임은 다음과 같다.

- 운영자에게 정상적인 활동 및 비정상적인 활동에 대한 적절한 훈련을 제공한다.
- 변경사항에 대한 리스크 평가를 요구하는 MOC(변경관리) 절차를 준수하거나 안전 관리가 그렇게 하고 있는지 확인한다. 리스크 평가를 활용하여 프로세스를 감독하고 플랜트 및 운영 절차에서의 리스크 컨트롤을 설계하고 구현한다.
- 작업 지침을 준비(또는 최소한 검토)한다. 그 지침이 안전하고 준수되는지 확인한다.
- 턴어라운드 과정과 같이 리스크가 높은 작업 중 리스크 주변의 인원을 최소화한다.
- 사건 및 교훈에 대한 기록을 유지하여 그것들로부터 학습해야 하는 사람들에게 전달하여 활용되도록 한다.
- 활동에 필요한 경험과 훈련을 갖춘 인력을 할당한다.
- 운영자들의 중요 활동 수행을 지원하는 프로세스 컨트롤 시스템을 제공한다.
- 감사를 실시한다. 감사(및 다른 피드백 소스)에 사용할 선행지표를 선정하거나 안전 엔지니어링에서 적절한 선행지표를 식별하였는지 확인한다.

운영 관리 인력의 프로세스 모델 결함

Process Model Flaws of operations management personnel

- Regarded ethylbenzene as a safe substance (an inert medium) under all process conditions. Therefore, they did not consider the heating phase to be risky.
- Thought the personnel involved in the turnaround had appropriate training and experience.
- Did they not know about similar incidents at other Shell installations with the same design or did they not think they were relevant to Unit 4800?
- In general, they had an inaccurate view of the risk that existed in the plant.
- Inadequate feedback leading to these flaws:
  - The heating phase did not appear in the report provided by plant safety management.
  - Plant safety management did not provide correct risk assessments to operations management.

Contextual Factors: (omitted, see complete analysis; also included in summary below)

Summary of the Role of Operations Management in the Accident:

- Operations management did not identify the flaws in the risk analyses performed or the procedures used for these risk analyses. The risk analyses complied with the minimal requirements of the Dutch regulatory authorities and apparently with the Shell requirements.
- Changes over time were not subjected to assessment in accordance with the MOC procedures.
- Work instructions were created by the operators without safety engineering oversight. They did not comply with the required Shell format for such work instructions and did not include important criteria for the job such as heating rate. Nitrogen flow, an important factor in the accident, was ignored in the work instructions.
- A decision was made to configure the process control system to control the plant during the normal production phase but not during non-production and maintenance phases. They did not think these activities were high risk and thought that manual operation would suffice. The reasons for this decision are not in the accident report.
- Two employees from different contractors were allowed to work in the adjacent unit during the start-up, probably because they did not believe that phase was dangerous.
- Operations management did not assign operators to the start-up that had the qualifications required in the Safety Report. No reason is given in the accident report as to why this happened.
- Operations management did not ensure that lessons learned from similar plants and at Shell Moerdijk in 1999 were incorporated in the design and operation of Unit 4800.
- The Safety Management System at Shell Moerdijk did not prevent unsafe situations from being overlooked or internal procedures from not being followed. There is no information in the accident report about who created the SMS or who was responsible for ensuring that it was working properly.
- Internal Shell Moerdijk audits did not show any of these shortcomings. Not enough information is provided to determine why they were ineffective.
- Shell Moerdijk has a Business Management System in which safety management is integrated. No details are provided, but in general this is a poor practice and has been a factor in major petrochemical company accidents such as Deepwater Horizon. Decision making needs to occur with full information about all the factors that must be considered and not lost by integrating risk information in a nontransparent way.

- 모든 프로세스 조건하에서 에틸벤젠이 안전한 물질(불활성 매체)로 간주된다. 이 때문에 운영 관리 인력들은 가열 단계가 위험하다고 생각하지 않았다.
- 턴어라운드에 관련된 인력은 적절한 훈련을 받았고 경험을 가지고 있다고 생각했다.
- 그들은 같은 설계를 가진 다른 쉘 설비의 유사 사고에 대해 몰랐거나 그 사고가 Unit 4800과 관련이 없다고 생각했는가?
- 일반적으로 그들은 플랜트에 존재하는 리스크에 대해 잘못된 견해를 가지고 있었다.
- 다음과 같은 결함으로 이어지는 부적절한 피드백
  - 플랜트 안전 관리의 보고서에는 가열 단계가 명시되지 않았다.
  - 플랜트 안전 관리는 운영 관리에 대한 올바른 리스크 평가를 하지 않았다.

컨텍스트적 요인 : (생략함, 완성된 분석 결과 참조; 아래 요약에도 포함됨)

사고에서의 운영 관리 역할 요약:

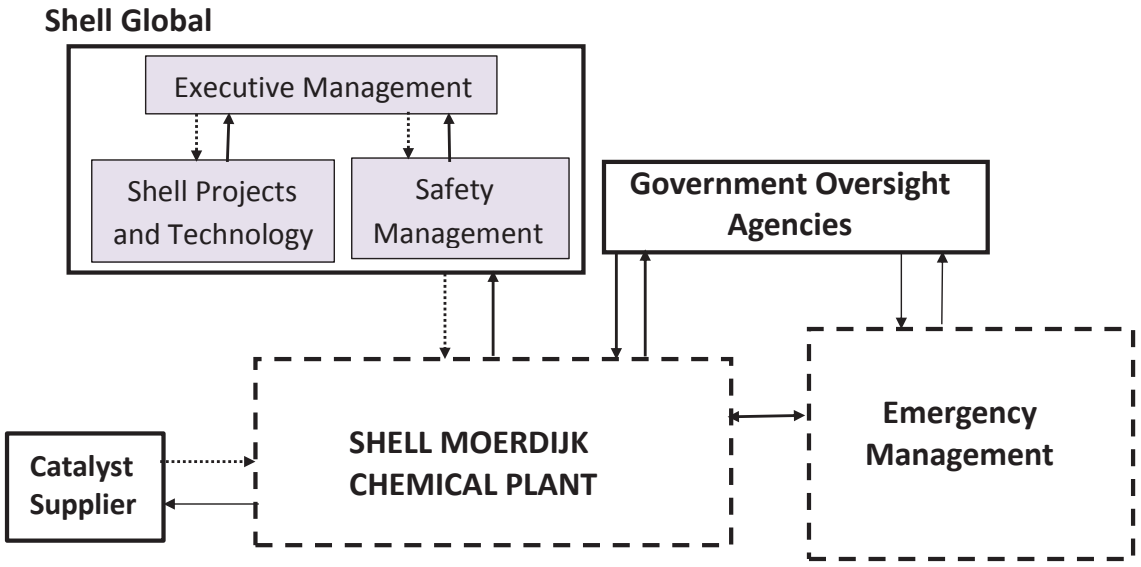
- 수행된 리스크의 분석 또는 이러한 리스크 분석에 사용되는 절차의 결함을 운영 관리에서 식별하지 못했다. 수행된 리스크 분석은 네덜란드 규제 당국의 최소한의 요구사항과 쉘의 요구사항을 준수하였다.
- 시간에 따른 변경사항이 변경관리(MOC) 절차에 따라 평가되지 않았다.
- 운영자가 안전 엔지니어링 감독 없이 작업 지침을 만들었다. 그들은 그러한 작업 지침 작성 시 쉘에서 요구하는 형식을 준수하지 않았으며 가열율과 같은 업무의 중요한 기준을 포함시키지 않았다. 사고의 중요한 요인인 질소 흐름은 작업 지침에서 무시되었다.
- 프로세스 컨트롤 시스템을 구성하여 플랜트를 컨트롤 하는 것을 정상적인 생산 단계에만 적용하기로 하였으며 비생산 및 유지보수 단계에서는 적용하지 않기로 결정했다. 그들은 이러한 활동이 리스크가 높다고 생각하지 않았으며 수동 작업으로도 충분하다고 생각했다. 이 결정에 대한 근거는 사고 보고서에 없다.
- 서로 다른 계약업체 직원 두 명이 기동 과정 중 인접한 장치에서 작업하고 있었다. 아마도 그 단계가 위험하다고 생각하지 않았기 때문일 것이다.
- 운영 관리는 안전 보고서에서 요구하는 자격을 갖춘 운영자를 기동 작업에 할당하지 않았다. 사고 보고서에는 왜 이런 일이 일어났는지에 대한 이유가 없다.
- 운영 관리는 유사한 플랜트 및 1999년 쉘 뫼르딕에서의 교훈이 Unit 4800의 설계 및 작업에 반영되도록 하지 못했다.
- 쉘 뫼르딕의 안전 관리 시스템은 안전하지 않은 상황이 간과되거나 내부 절차가 준수되지 않는 것을 방지하지 못했다. 사고 보고서에는 누가 SMS를 구축하였는지 또는 그 시스템의 정상 작동을 확인할 책임이 누구에게 있는지 대한 정보가 없다.
- 쉘 뫼르딕의 내부 감사는 이런 결점을 전혀 밝혀내지 못하였다. 그러한 것들이 왜 효과가 없었는지 판단하기 위한 정보가 충분히 제공되지 않았다.
- 쉘 뫼르딕에는 안전 관리가 통합된 사업 관리 시스템이 있다. 자세한 내용은 제공되지 않지만 일반적으로 이것은 잘못된 것이며 딥워터 호라이즌(Deepwater Horizon)과 같은 주요 석유 화학 기업 사고의 한 요인이었다. 의사결정은 고려되어야 하는 모든 요인에 대한 완전한 정보에 의해 기반하여 이루어져야 하며, 이 때 리스크에 대한 정보를 투명하지 않은 방식으로 통합하여 고려해야 할 요인이 손실되게 해서는 안 된다.

Recommendations:

- Establish and ensure proper MOC procedures are followed. If changes occur, retest assumptions that could be affected by those changes. This implies that these assumptions must be recorded, leading indicators established for identifying when they may no longer be correct, and a process established for testing and responding to changes that might affect these assumptions.
- A thorough review of the Shell Moerdijk SMS should be done with emphasis on why it was unable to prevent this accident. Major factors in this accident are related to basic activities that should have been controlled by the SMS.
- Update procedures to eliminate the causes of the accident such as lack of control and supervision of the work instruction creation and oversight processes, inadequate hazard analysis and risk assessment procedures, assignment of operators to perform the turnaround who did not have the required skills and expertise, inadequate use of lessons learned from the past, and audit procedures that did not identify the shortcomings before the accident.
- Improve the process control system to provide appropriate assistance to operators performing functions that are outside of normal production.

## Shell Global (Corporate)

Three basic functions are included here: Engineering design (Shell Projects and Technology), corporate safety management, and executive-level corporate management, including the Board of Directors. The exact distribution of the safety responsibilities in the Shell Global management structure was not included in the accident report, so they may be distributed throughout the Shell Global management structure differently than assumed here. The bottom line is that they need to be somewhere.




## Shell Projects and Technology (Engineering)

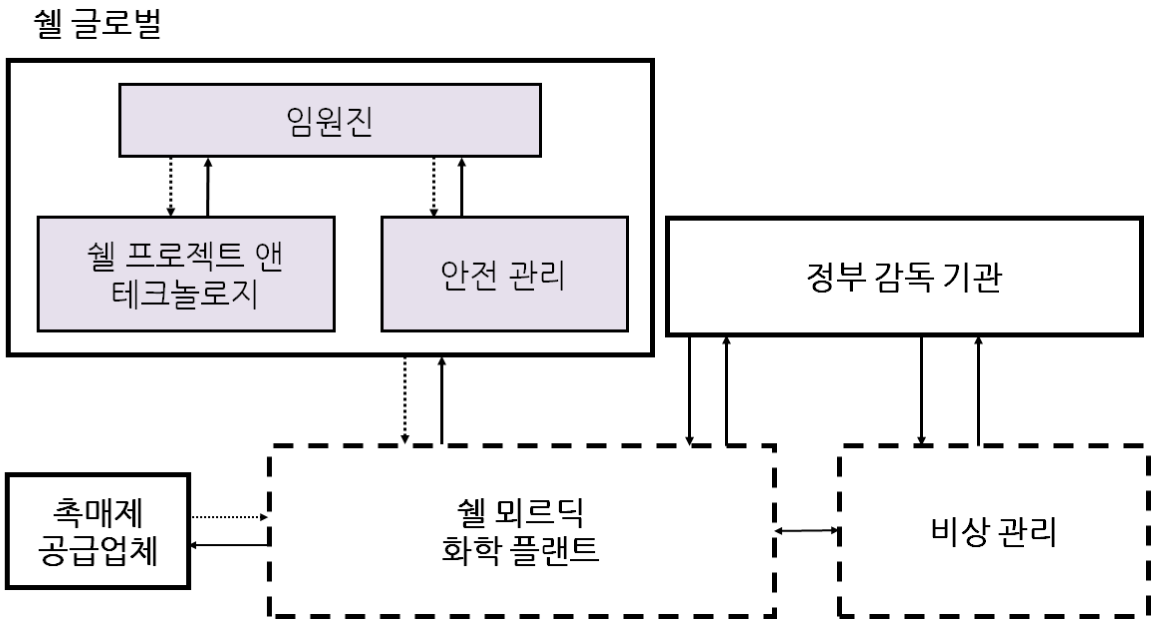
Plant design was done at the corporate level and the technology licensed to the facilities.

권고사항:

- 적절한 변경관리(MOC) 절차를 수립하고 준수하도록 한다. 변경사항이 있는 경우 그 변경사항에 영향을 받을 수 있는 가정을 재검증(retest)한다. 이것은 가정이 기록되어야 하고 그러한 가정이 더 이상 맞지 않는 시점을 식별하기 위해 선행지표를 확립해야 함을 의미한다. 또한 가정에 영향을 미칠 수 있는 변경사항을 테스트하고 대응하기 위해 프로세스를 확립해야 함을 의미한다.
- 쉘 뫼르딕의 SMS에 대한 철저한 검토는 이 사고를 방지할 수 없었던 이유에 중점을 두고 이루어져야 한다. 이 사고의 주요 요인은 SMS가 컨트롤해야 했던 기본적인 활동과 관련이 있다.
- 업무 지침의 생성과 감독 프로세스에 대한 컨트롤과 감독의 부족, 부적절한 위험 분석 및 리스크 평가 절차, 턴어라운드 수행에 필요한 기술과 전문성이 없는 운영자의 배정, 과거로부터 배운 교훈의 부적절한 활용, 사고 발생 전에 결점을 확인하지 못한 감사 절차 등의 사고 원인을 제거하기 위해 절차를 업데이트한다.
- 프로세스 컨트롤 시스템을 개선하여 정상적인 생산 절차 외의 작업을 수행하는 운영자에게 적절한 지원을 제공한다.

### 쉘 글로벌(기업)

여기에는 세 개의 기본적인 기능이 포함된다: 엔지니어링 설계(쉘 프로젝트 앤 테크놀로지), 기업 안전 관리, 이사회를 포함하는 경영진의 기업 관리. 쉘 글로벌 관리 구조의 안전 책임에 대한 정확한 분배는 사고 보고서에 포함되지 않았으므로, 여기서 가정한 것과는 다르게 쉘 글로벌 관리 구조 전체에 분배될 수 있다. 결론은 그 책임이 어딘가에는 있어야 한다는 것이다.




### 쉘 프로젝트 앤 테크놀로지 (엔지니어링)

플랜트는 기업 차원에서 설계되었으며 시설에 대한 기술은 라이선스를 받았다.

Safety-Related Responsibilities

- Create a safe design: Perform hazard analysis (or use the results of hazard analysis created by another group) and eliminate or mitigate the hazards in the design.
- Provide design, hazard, and operating information to the plant operators to help those who are operating the plants avoid any hazardous scenarios that the designers were not able to eliminate or adequately mitigate in the design itself.
- Learn from the operation of their designs and improve the designs based on this feedback.

Summary of the Role of Shell Projects and Technology:

The design data provided to the licensees was not usable by those creating work instructions at the plants. The design had safety-critical design flaws that were not found in hazard analyses during the initial design phase. These flaws were not fixed after receiving information about related incidents in other Shell plants. One example was an overpressure incident that occurred due to an inadequate number of temperature sensors and pressure relief valves unable to handle the excessive pressure that occurred. Unsafe and incomplete work instructions were approved by Shell Projects and Technology for the Unit 4800 turnaround at Shell Moerdijk.

Unanswered Questions:

Without more information about the operations at Shell Corporate, which was not included in the accident report, it is difficult to determine exactly why the unsafe control occurred. More questions than answers arise from the CAST analysis, such as *Why were the design flaws introduced and how did they get through the design process? What type of hazard analysis is performed by Shell Projects and Technology or by other groups? Why were identified design flaws not fixed after the incidents at Shell Moerdijk in 1999 and Nanhai in 2011? What other types of feedback is provided about the safety of their designs during operations in the Shell plants? What information about the safety aspects (hazards) of the plant design are passed from Shell Projects and Technology to the licensees of their designs? What information is included in the design book? Is the design data provided sufficient for the licensees to create safe work instructions if engineers are writing the work instructions instead of operators and did they not know who was going to be performing this task? Why did they approve unsafe work instructions that did not even follow the required Shell format? What information is provided in the Design Book about start-up and the hazards of start-up? What types of hazard analyses are performed during the design process? What is the process for ensuring safety when changes are made? How are safety-related assumptions recorded and what triggers a re-analysis of these assumptions? What feedback do the designers get about the operation of their designs?*

Recommendations:

Fix the design features contributing to accident. Determine how these flaws got through the design process and improve both the design and the design review processes. Fix the design book so that is understandable by those who are writing the work instructions and includes all the information needed to safely operate installations of the licensed technology. Fix the work instruction review process by Shell Projects and Technology to ensure the instructions are complete and safe. Review and improve the hazard analysis process used by Shell Projects and Technology.

안전 관련 책임

- 안전한 설계를 생성한다: 위험 분석을 수행(또는 다른 그룹이 만든 위험 분석 결과 사용)하고 설계의 위험을 제거하거나 완화한다.
- 플랜트 운영자에게 설계, 위험 및 운영 정보를 제공하여 설계에서 제거하거나 적절히 완화하지 못한 위험 시나리오를 피할 수 있도록 한다.
- 이 피드백을 바탕으로 설계에 대한 운영으로부터 학습하고 관련 설계를 개선한다.

쉘 프로젝트 앤 테크놀로지의 역할 요약

플랜트에서 작업 지침을 작성하는 사람들은 인허가를 받은 사용자에게만 제공되는 설계 데이터를 사용할 수 없었다. 그 설계에는 초기 설계 단계의 위험 분석 시에는 발견되지 않은 안전-중요 설계 결함이 있었다. 이러한 결함은 다른 쉘 플랜트에서 관련 사고에 대한 정보를 제공받은 후에도 수정되지 않았다. 한 가지 예로, 과압 사고가 있다. 이 사고는 온도 센서의 개수가 부족하고 압력 완화 밸브가 과압을 조절하지 못하여 발생하였다. 쉘 프로젝트 앤 테크놀로지는 쉘 뫼르딕의 Unit 4800 턴어라운드에 대한 안전하지도 완전하지도 않은 작업 지침을 승인하였다.

답변되지 않은 질문:

사고 보고서에도 포함되지 않았던 쉘 기업의 운영에 대한 추가 정보가 없다면 안전하지 않은 제어가 발생한 이유를 정확하게 파악하기가 어려울 것이다. CAST 분석 과정에서는 다음과 같이 답변보다 더 많은 질문이 생긴다. *설계 결함이 왜 유입되었고 어떻게 설계 프로세스를 통과했는가? 쉘 프로젝트 앤 테크놀로지나 다른 그룹이 수행한 위험 분석은 어떤 유형인가? 1999년 쉘 뫼르딕과 2011년 난하이에서 발생한 사고 이후에도 수정되지 않았던 설계 결함이 왜 식별되었는가? 쉘 플랜트 운영 중의 설계 안전에 대한 어떤 다른 유형의 피드백이 제공되는가? 쉘 프로젝트 앤 테크놀로지는 그들의 라이선스를 사용하는 사용자에게 플랜트 설계의 안전 측면(위험)에 대해 어떤 정보를 알려주는가? 설계서에는 어떤 정보가 포함되어 있는가? 엔지니어가 이 작업을 누가 수행하는지 모르는 상태에서 운영자 대신 작업 지침을 작성하는 경우, 라이선스 사용자가 안전한 작업 지침을 생성할 수 있도록 충분한 설계 데이터를 제공하는가? 왜 그들은 쉘의 형식조차 따르지 않는 안전하지 않은 작업 지침을 승인했는가? 설계서에서 기동 및 기동의 위험에 대한 어떤 정보를 제공하는가? 설계 과정에서 어떤 유형의 위험 분석이 수행되는가? 변경사항이 있는 경우 안전을 보장하기 위한 프로세스는 무엇인가? 안전-관련 가정은 어떻게 기록되고 있으며 이러한 가정의 재분석은 어떤 기준으로 수행(트리거)되는가? 설계자들은 설계한 것이 운영될 때 어떤 피드백을 받는가?*

권고사항:

사고에 기여하는 설계의 특성을 개선한다. 이러한 결함이 설계 프로세스를 어떻게 통과했는지 파악하고 설계 및 설계 검토 프로세스를 모두 개선한다. 설계서를 수정하여 작업 지침을 작성하는 사람들이 이해하기 쉽게 하고 라이선스 받은 기술의 안전한 운영에 필요한 정보를 모두 포함하도록 한다. 쉘 프로젝트 앤 테크놀로지의 작업 지침 검토 프로세스를 수정하여 지침이 완전하고 안전하게 한다. 쉘 프로젝트 앤 테크놀로지에서 사용하는 위험 분석 프로세스를 검토 및 개선한다.

## Corporate Safety Management

There is no mention in the accident report about a Shell corporate safety program or about any of its potential contributions to the accident. In the CAST analysis, I took the information about what happened at the local Shell Moerdijk level and projected what would normally be the responsibility at the corporate level of a well-designed SMS to control the flawed safety activities. There must have been someone with ultimate responsibility for safety at the corporate level, but it is unclear where the activities associated with that management role resided within the corporate structure or even whether these activities occurred.

Relevant Responsibilities

- Ensuring the safety of the plant design, including the conduct of hazard analysis on designs licensed to subsidiaries.
- Oversight of operational safety at the various Shell plants and facilities.
- Management of change procedures related to safety: creating them, making sure they are followed, and improving them using feedback from incidents.
- Ensuring communication among separate plants in different parts of the world about incidents, lessons learned, etc.
- Creating and updating a Shell-wide Safety Information System and ensuring the information is being communicated adequately both within Shell Corporate and globally and that it is complete and usable.

Summary of the Role of Corporate Safety Management: There appears to have been a flawed view of the state of risk and the effectiveness of the safety management system in local Shell plants. The flawed process model is most likely related to inadequate feedback (including audits and leading indicators). The accident report says that Shell uses the outdated HEMP and bow tie model. There is little information about what other hazard analyses and risk assessments are used at the corporate level. Presumably HAZOP is also practiced (as in most of the process industry), but that is not mentioned in the report. Bow tie, which is about 60 years old and dates back to the late 60s, uses a simple chain-of-events model and is too simplistic to capture the hazards and risks in today's complex systems, including chemical plants. Once again, many questions are raised from the CAST analysis that need to be answered to understand the role of corporate level safety management in the accident and thereby to provide more effective safety management in the future.

Recommendations: Improve Shell safety audits. Review all risk assessment and hazard analysis processes and, in general, improve their approach to safety with respect to both safety analysis and safety management. Shell is not alone among the large oil companies in needing to update their methods. The petrochemical industry has too many accidents and incidents that are avoidable.

More specifically, the accident report says that Shell should "evaluate how risk analyses are performed and make changes. This should include procedures and policies about re-evaluation of earlier presumptions and assumptions. Conduct new risk analyses, put adequate measures in place, and ensure that the team that performs these analyses has sufficient critical ability. Pay particular attention to assumptions based on risks that had previously been ruled out."

Evaluate and improve the corporate safety management system. Improve procedures for learning from process safety-related incidents. Create better feedback mechanisms, including audits and leading indicators, and procedures for learning from incidents.

### 기업 안전 관리(Corporate Safety Management)

사고 보고서에는 쉘 기업의 안전 프로그램이나 사고의 잠재적 기여에 대한 내용은 언급되어 있지 않다. 필자는 CAST 분석 과정에서, 로컬 쉘 뫼르딕 수준에서 발생한 것에 대한 정보를 수집하였고 결함 있는 안전 활동을 컨트롤하기 위해 잘 설계된 SMS가 기업 차원에서 어떤 책임이 있는지를 보았다. 기업 차원에서 안전에 대해 궁극적으로 책임을 지는 사람이 있었을 것이지만 기업 구조의 어느 곳에 그 관리 역할과 관련된 활동이 있었는지 또는 이러한 활동이 발생했는지 여부 조차도 불분명하다.

관련 책임

- 자회사에 라이선스를 준 설계에 대한 위험분석 수행을 포함한 플랜트 설계의 안전을 보장한다.
- 다양한 쉘 플랜트 및 시설에서의 운영 안전을 감독한다.
- 안전과 관련된 변경절차 관리: 변경절차를 만들고 그 절차를 준수하는지 확인하며 사건으로부터의 피드백을 통해 변경절차를 개선한다.
- 사건, 교훈 등에 대해 세계 각지의 플랜트 간에 의사소통한다.
- 광범위한 쉘 안전 정보 시스템을 구축하고 업데이트하여 그 정보가 쉘 기업 및 전 세계적으로 적절히 전달되게 하고, 완전하며 사용 가능하도록 한다.

기업 안전 관리 역할 요약: 로컬 쉘 플랜트에서 리스크의 상태와 및 안전 관리 시스템의 효과에 대한 잘못된 관점이 있었던 것으로 보인다. 결함 있는 프로세스 모델은 부적절한 피드백(감사 및 선행지표 포함)과 관련이 있을 것이다. 사고 보고서에 따르면 쉘은 오래된 HEMP (Hazard Effect Management Process)와 보우 타이(Bow tie) 모델을 사용한다고 한다. 기업 차원에서 다른 위험 분석 및 리스크 평가가 사용된다는 정보는 거의 없다. 아마 HAZOP도 수행되었겠지만(대부분의 프로세스 산업에서와 같이) 보고서에는 언급되지 않는다. 1960년대 후반부터 약 60년 정도 된 보우 타이 모델은 단순한 이벤트 체인 모델을 사용하며 화학 플랜트와 같은 오늘날의 복잡한 시스템의 위험과 리스크를 파악하기에는 너무 단순하다. 다시 언급하지만, 사고에 대한 기업 차원의 안전 관리 역할을 이해하고 그로 인해 향후 보다 효과적인 안전 관리를 제공하기 위해 답변해야 하는 많은 질문들이 CAST 분석을 통해 제기될 수 있다.

권고사항: 쉘 안전 감사를 개선한다. 모든 리스크 평가 및 위험 분석 프로세스를 검토하고 안전 분석 및 안전 관리와 관련된 접근 방식을 전반적으로 개선한다. 대형 석유 회사들 중에서 접근 방식을 업데이트해야 하는 회사는 쉘만이 아니다. 석유 화학 산업에는 피할 수 있는 사고 및 사건이 매우 많다.

보다 구체적으로 사고 보고서에서는 쉘이 “리스크 분석이 어떻게 수행되었는지 평가하고 이를 개선해야 한다. 여기에는 이전의 추정 및 가정의 재평가 절차와 정책이 포함되어야 한다. 새로운 리스크 분석을 수행하고 적절한 조치를 취하며, 분석을 수행하는 팀이 충분한 핵심 능력을 갖출 수 있도록 한다. 과거에 누락된 리스크에 기반하는 가정에 특히 주의해야 한다.” 라고 명시하고 있다.

기업의 안전 관리 시스템을 평가하고 개선한다. 프로세스 안전-관련 사건으로부터 학습하기 위한 절차를 개선한다. 감사 및 선행지표, 사고로부터 학습하는 절차 등 보다 나은 피드백 메커니즘을 생성한다.

## Executive-Level Corporate Management

Responsibilities:

- Take all measures necessary to
  - Prevent major accidents from occurring and,
  - If accidents do occur, mitigate their consequences for humans and the environment
- Ensure the health and safety of the employees in relation to all aspects associated with the work (based on the Working Conditions Act and other regulations)
- Follow the government regulations in the countries where their plants are located.
- Create an effective safety management system and establish a strong safety culture policy. Ensure that the SMS and safety policies are being followed and they are effective.

Process Model Flaws

Leaders clearly had misunderstandings about the state of safety being practiced in Shell corporate and the local installations and the effectiveness of their defined procedures.

Contextual Factors (omitted, see full analysis):

Summary of the Role of Executive-Level Management:

Corporate management is responsible to ensure that an effective safety management system is created. Typical policies of an effective safety management system were violated at both Shell Corporate and Shell Moerdijk. The group overseeing safety at the Shell corporate level was clearly not effective. There is nothing included in the accident report about the assigned safety-related responsibilities for corporate management.

There is also nothing included in the accident report about context that might explain why standard executive-level responsibilities for safety were not effectively carried out. There seems to be a safety culture problem at Shell. (See later analysis of the safety culture and high-level safety policy at Shell.) What is the culture of the chemical industry in terms of corporate management oversight of the safety of global installations?

The accident report notes that the Safety Management System was integrated with the Business Management System at Shell Moerdijk. Was this also true at the corporate level? This is a very poor practice (and was a factor in the Deepwater Horizon accident). Safety risk assessments need to be kept separate from business risk assessments so that information is not hidden from high-level decision-makers.

Recommendations: Review the SMS design and determine why it did not prevent obvious violations of policy such as shortcomings in safety studies, management of change procedures, learning from accidents, not following regulations (e.g., having experienced operators and following the format for work instructions). Determine why audits were not effective in finding such obvious procedural noncompliance. While it is possible that this was the first time such lapses have occurred, it is highly unlikely. Strengthen audit procedures, including identifying better leading indicators of increasing risk than simply the number of leaks and create other forms of feedback to identify when the safety management system is drifting off course and risk is increasing. Establish better feedback channels to ensure that management of change procedures and corporate safety policy are being followed.

### 경영진의 기업 관리(Executive-Level Corporate Management)

책임 :

- 다음에 필요한 모든 조치를 취한다.
  - 중대한 사고의 발생을 방지하고,
  - 사고 발생 시 해당 사고가 사람 및 환경에 미치는 영향을 완화한다.
- 업무와 관련된 모든 측면에 대해 직원의 건강과 안전을 보장한다(근로조건법 및 기타 규정에 따라)
- 플랜트가 위치하고 있는 국가의 정부 규정을 준수한다.
- 효과적인 안전 관리 시스템(SMS)을 구축하고 강력한 안전 문화 정책을 수립한다. SMS와 안전 정책이 준수되고 있으며 효과적인지 확인한다.

프로세스 모델 결함

리더들은 쉘 기업과 지역 시설의 안전 상태 및 규정 절차의 효과에 대해 명백하게 오해하고 있었다.

컨텍스트적 요인 (생략함, 전체 분석 참조) :

경영진의 역할 요약:

기업 경영진은 효과적인 안전 관리 시스템을 구축할 책임이 있다. 효과적인 안전 관리 시스템의 일반적인 정책은 쉘 기업과 쉘 뫼르딕 모두에서 위반되었다. 쉘 기업 차원에서 안전을 감독하는 그룹은 명백히 효과적이지 않았다. 사고 보고서에는 기업 경영진에 할당 된 안전 관련 책임에 관한 내용이 포함되어 있지 않았다.

사고 보고서에는 안전에 대한 경영진의 일반적(standard) 책임이 효과적으로 이행되지 않은 이유를 설명할 수 있는 컨텍스트 대한 내용도 없었다. 쉘에는 안전 문화의 문제가 있는 것으로 보인다. (쉘의 안전 문화 및 상위 수준의 안전 정책에 대한 이후 분석 참조.) 글로벌 설비의 안전에 대한 기업의 관리 감독 측면에서 화학 산업의 문화는 무엇인가?

사고 보고서에 따르면 안전 관리 시스템은 쉘 뫼르딕의 비즈니스 관리 시스템과 통합되었다. 기업 차원에서도 이것이 사실일까? 이것은 매우 좋지 않은 관행이다(이는 딥워터 호라이즌 사고의 한 요인이었다). 안전 리스크 평가는 비즈니스 위험 평가와 별도로 분리하여 정보가 상위 의사결정자에게 숨겨지지 않도록 해야 한다.

권고사항: SMS 설계를 검토하여 정책을 명백하게 위반한 이유를 파악한다. 그 이유에는 안전 연구, 변경절차 관리, 사고로부터 학습의 결점, 규정 (예: 경험 있는 운영자를 고용하고 업무 지침 형식을 따르는 것) 미준수 등이 있다. 명백한 절차 불이행을 찾는 데 감사가 왜 효과적이지 않았는지 파악한다. 그러한 과실이 발생한 것이 처음일 수도 있지만 그럴 가능성은 매우 낮다. 단순히 누출 횟수를 식별하는 것보다는 리스크 증가에 대한 보다 나은 선행지표를 식별하고, 안전 관리 시스템의 이탈(drifting off) 및 리스크 증가 시기를 식별하기 위한 다른 형태의 피드백을 생성하는 등 감사 절차를 강화한다. 변경절차를 관리하고 기업의 안전 정책이 준수될 수 있도록 더 나은 피드백 채널을 구축한다.

## Catalyst Supplier

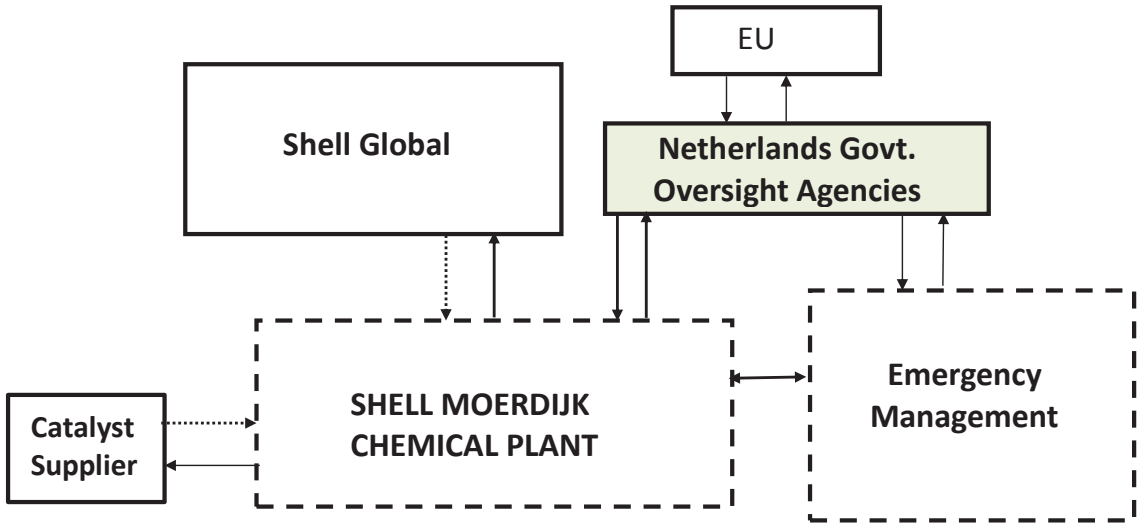
Safety-Related Responsibilities

- Provide information to customers that is needed to evaluate the use of their catalyst in the reactor being designed and/or operated
- Alert customers when changes are made in the catalyst that could potentially affect the safety of its use.

Summary of the Role of the Catalyst Manufacturer in the Accident: The changes made in the catalyst were not pointed out to Shell, but they were included in a new safety information sheet. While the catalyst manufacturer cannot determine the impact of their changes on a customer, the manufacturer should provide some clear alert that changes have been made and what they are so the customers are made aware of them.

Recommendations: Change contractual relationships between Shell and its suppliers to ensure that potentially critical changes are communicated appropriately. Make changes within information sheets so they are clear and obvious.

## Dutch Regulatory Authorities




All Dutch oversight safety and environmental authorities are grouped together here. There are two main policies:

1. Brzo: Companies must take all measures to prevent accidents and, if they occur, mitigate their consequences for humans and the environment. The company must implement this obligation

### 촉매제 공급 업체(Catalyst Supplier)

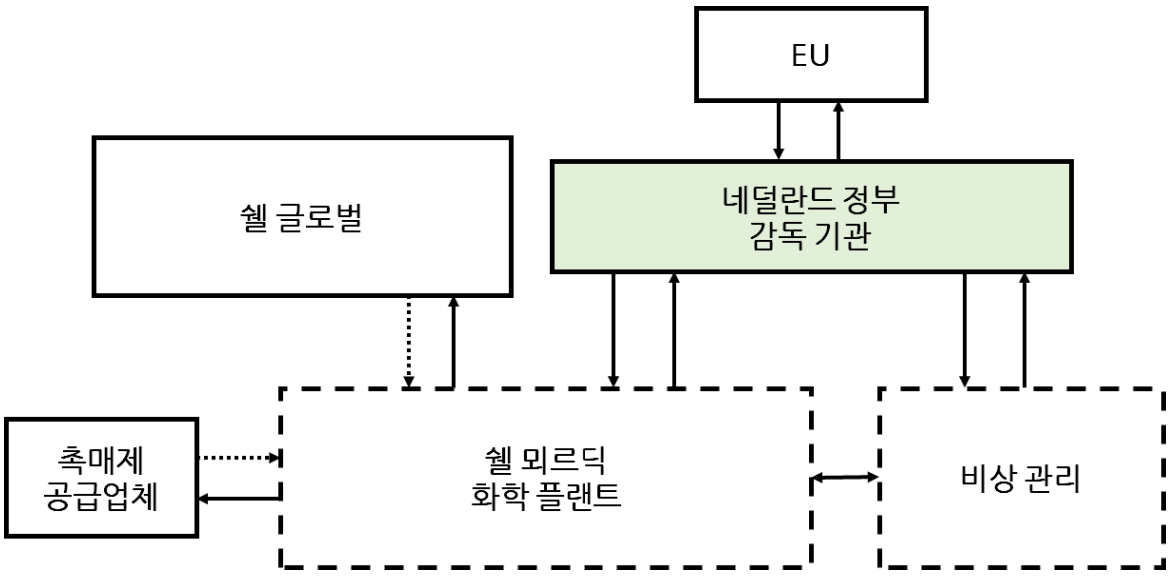
안전-관련 책임:

- 설계 및/또는 작동 중인 반응로에서 촉매제의 사용을 평가하는 데 필요한 정보를 고객에게 제공한다.
- 촉매제의 사용 안전성에 영향을 미칠 수 있는 변경이 있는 경우 고객에게 알린다.

사고에서 촉매제 제조업체의 역할 요약: 촉매제 제조업체가 촉매제의 변경사항을 쉘에게 지적하여 알리지는 않았지만 그 내용은 새로운 안전 정보 시트에 포함되었다. 촉매제 제조업체는 변경사항이 고객에게 미치는 영향을 파악할 수는 없지만 변경 여부 및 변경사항에 대해 명백히 알려서 고객이 인식할 수 있도록 해야 한다.

권고사항: 잠재적으로 중요한 변경사항이 적절하게 전달되도록 쉘과 공급 업체 간의 계약 관계를 변경한다. 정보 시트를 변경하여 그 변경사항이 명확하고 분명하도록 한다.

### 네덜란드 규제 당국(Dutch Regulatory Authorities)




모든 네덜란드의 안전 및 환경 감독 당국은 여기에 그룹화 되어 있다. 두 가지 주요 정책은 다음과 같다.

1. Brzo: 회사는 사고를 방지하기 위한 모든 조치를 취해야 하고 만약 사고 발생 시에는 사람과 환경에 미치는 영향을 완화해야 한다. 회사는 심각한 사고 예방 정책(PBZO)에 정책 가정을 세우고 안전 보고서(VR)를 작성하며 안전 관리 시스템의 구축을 통해 이러한 의무를 이행해

by laying down policy assumptions in the Prevention Policy for Serious Accidents (PBZO), drawing up a safety report (VR), and organizing a safety management system.

2. Wabo: Regulators must check whether the company complies with regulations connected to the environmental permit, i.e., environmental safety.

General Relevant Safety-Related Responsibilities

- Responsible for supervision and enforcement of Dutch laws to protect the environment and the public. Perform Brzo inspections focusing on process safety and Wabo inspections focusing on environmental safety.
- Responsible for enforcement of EU health and safety laws within the Netherlands.

More Specific Responsibilities:

- Identify shortcomings at companies they are responsible to oversee.
- Encourage companies to improve their safety-critical processes through supervision and enforcement. Identify shortcomings and require companies to investigate and detect deep-seated causes of incidents and accidents. Ensure that any shortcomings identified are corrected.
- Assess modifications made to plants, procedures, and processes (although they are not expected to perform the risk analyses for the companies).
- Pay greatest attention to safety-critical processes, including maintenance and reactor start-up.

Process Model Flaws

The accident report said "Regulators had a positive view of the Shell Moerdijk safety management system. A number of shortcomings at Shell Moerdijk did not alter this view."

Contextual Factors (omitted, see full analysis and summary below)

Summary:

At least partly because of limited resources, the government authorities do "system-related supervision," effectively a form of performance-based regulation where responsibility is placed on the operator of high-risk activities to identify their own shortcomings. Regulators check both the design and operation of the safety management system and perform annual inspections to ensure they are operating as designed. Regulators only ensure that companies have the right documented procedures and spot check that they are being used.

They did not notice or did not react to Shell not acting in accordance with its own SMS. As just some examples: Changes and upgrades to the plant were not consistently subjected to risk analyses (violating the Shell SMS requirements), but this deficiency was not noted by the regulators nor required to be fixed. Changes were not adequately evaluated for safety. Requirements for expertise and training in performing startups were not enforced.

The accident report implies that regulators gave Shell Moerdijk a pass on behavior that might have instead been labeled violations. Plant scenario deficiencies should have been considered a violation but were not. Scenarios were not up to date or were incomplete. Working under limited resources and time is difficult under any supervision model, but system-level supervision has major limitations in ensuring public safety. The accident investigation showed many flaws in Shell Moerdijk operations

야 한다.

2. Wabo: 규제 기관은 회사가 환경 허가(예: 환경 안전)와 관련된 규정을 준수하는지 확인해야 한다.

일반적인 안전 관련 책임

- 환경과 공공을 보호하기 위한 네덜란드 법률의 감독과 집행의 책임이 있다. 프로세스 안전에 초점을 둔 Brzo 조사와 환경 안전에 초점을 둔 Wabo 조사를 수행한다.
- 네덜란드 내 EU 보건 및 안전 법률의 시행을 책임진다.

보다 구체적인 책임:

- 감독해야 하는 회사의 결점을 파악한다.
- 감독과 이행을 통해 기업이 안전-중요 프로세스를 개선하도록 독려한다. 결점을 파악하고 기업이 사건과 사고의 심청적 원인을 조사 및 탐지하도록 요구한다. 식별된 결점이 모두 수정되었는지 확인한다.
- 플랜트, 절차, 프로세스 수정 사항을 평가한다(비록 회사에 대한 리스크 분석을 수행하지 않더라도).
- 유지보수 및 반응로 기동 등 안전-중요 프로세스에 최대한 주의한다.

프로세스 모델 결함

사고 보고서는 “규제기관들은 쉘 뫼르딕 안전 관리 시스템에 대해 긍정적인 견해를 가지고 있었다. 쉘 뫼르딕의 많은 결점들에도 이러한 견해는 바뀌지 않았다.“고 언급하였다.

컨텍스트적 요소(생략함, 아래의 전체 분석 및 요약 참조)

요약 :

정부 당국은 제한된 자원으로 인해 최소한 부분적으로라도 효과적인 “시스템 관련 감독”을 수행하는데, 이는 리스크가 높은 활동을 하는 운영자가 스스로 결점을 확인할 수 있도록 책임을 부여하는 성과 기반 규제의 한 형태이다. 규제 기관은 안전 관리 시스템의 설계 및 운영을 모두 점검하고 매년 점검을 실시하여 설계된 대로 작동하는지 확인한다. 규제 기관은 회사가 제대로 문서화된 절차를 보유하고 있는지 여부와 실제로 그것을 사용하는지에 대한 임의 조사를 수행한다.

그들은 쉘이 자신들의 SMS에 부합하게 행동하지 않는 것을 알아채지 못했거나 대응하지 않았다. 다음은 몇 가지 예이다: 플랜트의 변경 및 업그레이드 과정에서 리스크 분석을 계속 수행하지 않았다(쉘 SMS 요구사항 위반). 그러나 규제 기관은 이와 같은 결함을 언급하지 않았고 수정을 요구하지도 않았다. 안전에 대한 변경사항의 평가가 제대로 이루어지지 않았다. 기동 업무에 대한 전문성과 훈련 요구사항은 강제되지 않았다.

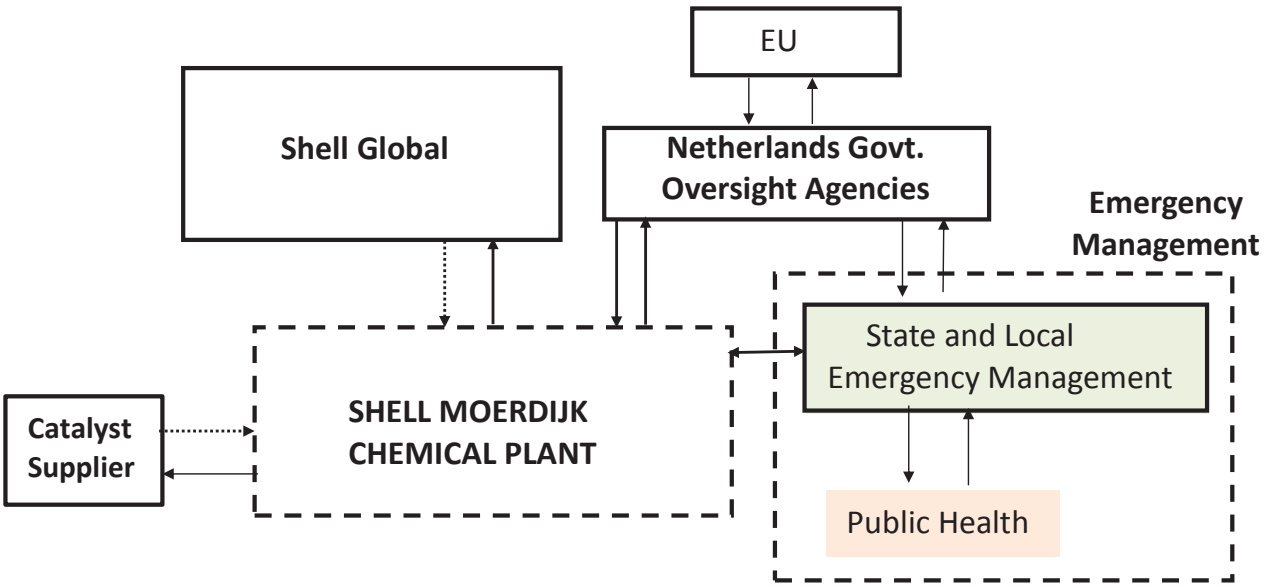
사고 보고서는, 규제 기관이 쉘 뫼르딕에게 위반으로 분류될 수도 있었던 행동을 넘어가 주었다고 암시하고 있다. 플랜트 시나리오의 결함은 위반으로 간주되어야 했지만 그렇지 않았다. 시나리오는 최신 버전이 아니었거나 완전하지 않았다. 제한된 자원과 시간 하에서 감독하는 것은 어떤 감독 모델이든 어려운 일이지만 시스템 수준의 감독으로 공공 안전을 보장하는 데 큰 한계가 있

safety management as defined and as implemented. *What is wrong with the supervision model that the regulators did not detect the deficiencies?*

Recommendations:

Better supervision of the highest risk activities is needed, including turnarounds. Regulators need to oversee and ensure that strict procedures are being used for the most dangerous activities and that the safety management system is operating effectively and following its own rules. Operating under limited resources does not preclude doing something effective, it simply requires a more intelligent selection of activities that are performed. There is a need for better evaluation procedures and oversight of safety management system effectiveness. The regulators should rethink system-level supervision to ensure that what they are doing is effective in preventing accidents like the Shell Moerdijk explosion.

## Emergency Services




Responsibilities

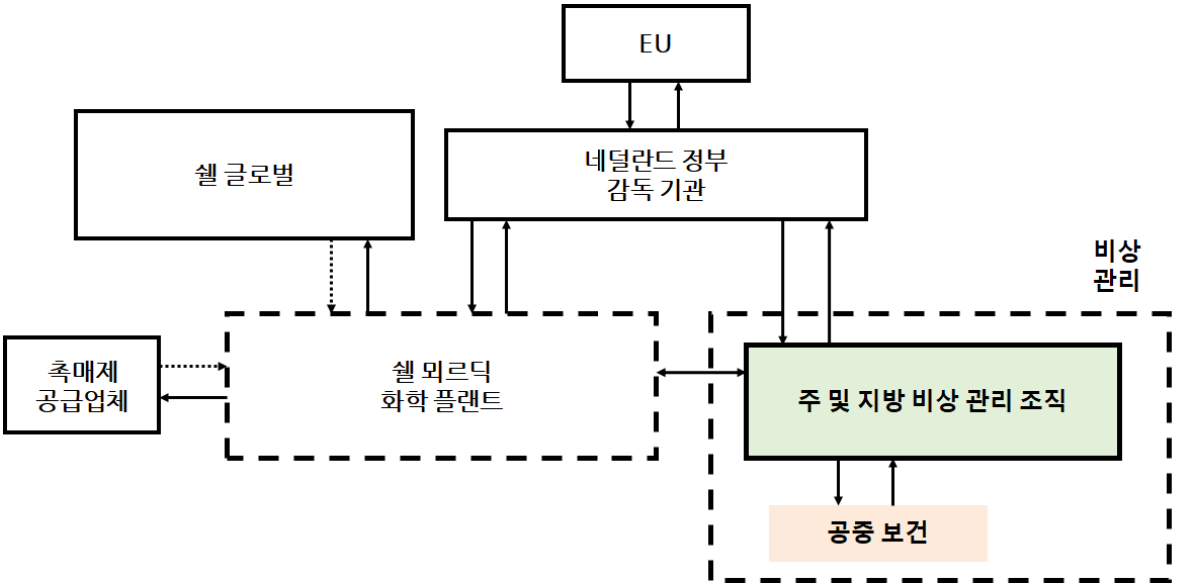
- Firefighting [collaborative fire brigades did this effectively in this case], crisis management, crisis communications including among other things:
  - Informing citizens of the incident
  - Measuring substances released on a coordinated basis
  - Operating a telephone advisory line
  - Informing citizens about the results of the measurement of the substances released and the ensuing recommendations.

다. 사고 조사는 쉘 뫼르딕의 운영 안전 관리에서 정의되고 구현된 있는 많은 결함들을 보여 주었다. *규제기관이 결함을 발견하지 못한 감독 모델의 문제점은 무엇인가?*

권고사항:

턴어라운드를 포함하여, 리스크가 매우 높은 활동에 대해 보다 나은 감독이 필요하다. 규제 당국은 매우 위험한 활동에 대해 엄격한 절차를 사용하도록 해야 하며 안전 관리 시스템이 효과적으로 작동하고 자체 규칙을 준수하도록 감독하고 강제해야 한다. 제한된 자원으로 운영한다고 해서 효과적으로 작업할 수 없는 것은 아니며, 수행할 활동을 보다 지능적인 선택하기만 하면 된다. 안전 관리 시스템의 효과에 대한 보다 나은 평가 절차 및 감독이 필요하다. 규제 당국은 쉘 뫼르딕 폭발과 같은 사고를 효과적으로 방지하기 위한 시스템 수준의 감독에 대해 다시 생각해보아야 한다.

### 비상 서비스 조직(Emergency Services)




책임

- 소방[이 사고에서는 공동 소방대가 효과적으로 수행하였음], 위기 관리, 아래 사항을 포함하는 위기 커뮤니케이션:
  - 시민들에게 사건을 알림
  - 조정된 기준에 근거하여 유출된 물질을 측정
  - 전화 상담 라인을 운영
  - 유출된 물질의 측정 결과와 그에 따른 권고사항을 시민들에게 알림

Summary of the Role of Emergency Services in the Accident:
Emergency services were mostly very effective in carrying out their responsibilities, but some deficiencies, particularly in communication, were uncovered in the accident response. For example, many people used WhatsApp instead of the National Crisis Management System designed for use in these conditions. It did not lead to loss of life because of the nature of the accident in this case, but under other circumstances it could have.

Recommendations: What was learned from this case should be used to improve the National Crisis Management System, including why many people used WhatsApp instead, and how the official system can incorporate those features.

Even for system components that did not cause a loss, as in this instance, accidents create an opportunity to look closely at the actual operation of our systems in times of stress and provide a learning opportunity that should not be wasted. As demonstrated in the example, most of the components may have contributed to the accident in some way or did not operate exactly as planned. When looking only at what the operators did or did not do, it appears that they were the primary contributors to the loss. Usually, as in this case, the actions of the operators will be found to be understandable when the reason for their behavior is examined.

This section described and provided examples of individual component analysis in CAST. Examining the individual controllers in the control structure is not enough, however. It is necessary to also examine the operation of the control structure as a whole.

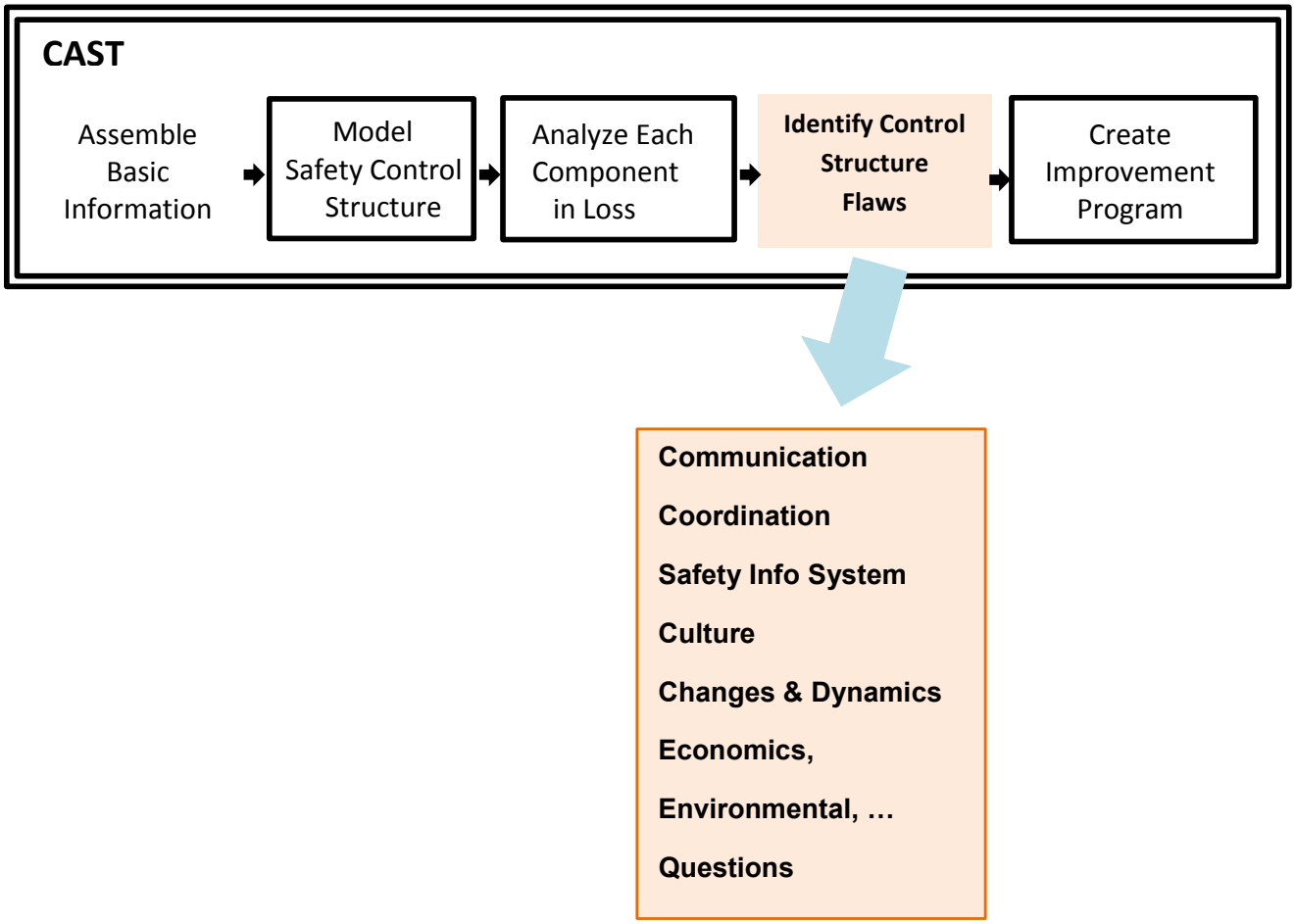
사고 시 비상 서비스 조직의 역할 요약:
비상 서비스 조직은 책임 수행에 있어 대부분 매우 효과적이었지만 사고 대응 과정에서의 일부 결점, 특히 의사소통에서의 일부 결점이 발견되었다. 예를 들면 이러한 조건에서 사용하도록 설계된 국가 위기관리 시스템(National Crisis Management System) 대신에 WhatsApp을 사용하는 사람들이 많았다. 이 사고의 경우 사고의 특성상 인명피해로 이어지지 않았지만 다른 상황이라면 인명피해가 발생했을 수 있다.

권고사항: 이 사례를 통해 배운 내용은, 많은 사람들이 WhatsApp을 대신 사용한 이유와 공식 시스템이 WhatsApp의 기능을 반영할 수 있는 방법과 함께 국가 위기관리 시스템의 개선에 활용되어야 한다.

이 사례에서와 같이 사고는 손실을 초래하지 않는 시스템 컴포넌트에 대해서도 비상상황에서 시스템이 실제 어떻게 동작하는지를 면밀히 살펴볼 수 있는 기회를 제공하며, 놓쳐서는 안 되는 학습 기회를 제공한다. 예시에서 알 수 있듯이 대부분의 컴포넌트는 어떤 식으로든 사고에 기여할 수 있으며 계획된 대로 정확하게 작동하지 않을 수 있다. 운영자들이 수행한 것과 수행하지 않은 것만을 본다면 그 운영자들이 주요 손실의 원인이었던 것처럼 보일 것이다. 일반적으로 이 사례에서와 같이 운영자가 그렇게 행동한 이유를 살펴본다면 그 행동이 이해할 수 있는 것임을 알게 될 것이다.

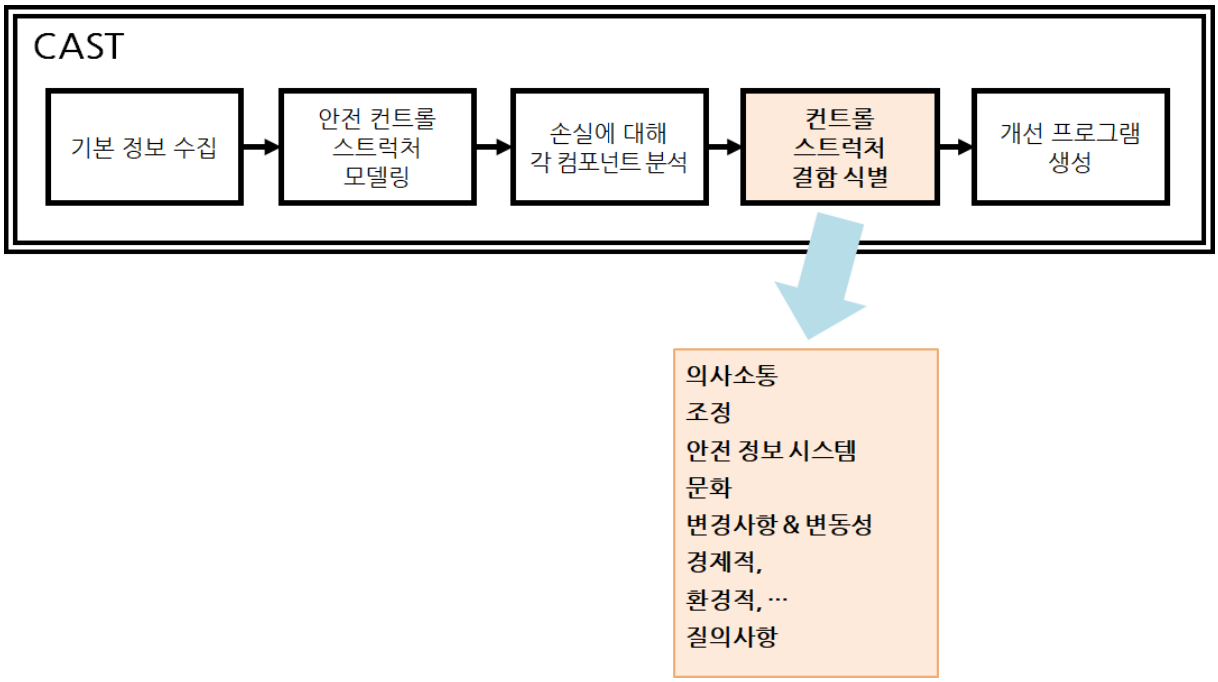
이 섹션에서는 CAST에서의 개별 컴포넌트 분석 사례를 제시하였다. 그러나 컨트롤 스트럭처의 개별 컨트롤러를 검토하는 것만으로는 충분하지 않다. 컨트롤 스트럭처의 동작을 전체적으로 검토할 필요가 있다.

## Analyzing the Control Structure as a Whole




4. *Identify flaws in the control structure as a whole by investigating the general systemic factors that contributed to the loss. The systemic factors span the individual system control structure components.*

## 전체로서의 컨트롤 스트럭처 분석




*4. 손실에 기여한 컨트롤 스트럭처의 결함을 전체의 관점(종합적인 시스템적 요인)에서 식별한다. 시스템적 요인은 시스템 컨트롤 스트럭처 컴포넌트 각각에 분포되어 있다.*

The CAST analysis process described so far focuses on individual system components and their control over other components. It examines why each of the controllers was unable to enforce the controls and constraints assigned to it.

In contrast, this part of CAST looks at the control structure as a whole and the systemic factors that led to the ineffectiveness of the designed controls. It is perhaps the least structured part of the analysis, but guidance is provided in this section of the handbook on what to look for and how to explain the role it played when you find it.

The systemic analysis focuses on factors that affect the behavior and interactions of all the components working together within the safety control structure to prevent hazardous system states. By looking at the system as a whole, rather than individual components, we can identify causal factors that impact how the various safety control structure components interact. These systemic factors provide another way to understand why the individual components may not fulfill their individual safety responsibilities and why together their behavior did not satisfy the system safety constraints. That is, safety control structures are usually created so that one component's misbehavior cannot alone lead to an accident. The systemic causal factors, however, can negatively impact the behavior of many or even all of the components and defeat these efforts.

This is the truly unique part of a systems approach to accident analysis that is omitted from event-based models, such as the Swiss Cheese or domino models. There are causal factors that can prevent all the barriers from operating correctly and simultaneously cause "holes" in all the protections and cheese slices that were created to prevent accidents. Getting away from focusing on a few causal factors or explaining accidents in terms of the behavior of one or several components provides a larger view of causality that can be used to identify very powerful prevention measures.

The following are some of the systemic factors that might be considered. This list is not comprehensive, but simply a starting point.

- Communication and coordination
- The safety information system
- Safety culture
- Design of the safety management system
- Changes and dynamics over time: in the system and in the environment
- Internal and external economic and related factors in the system environment not covered previously in the analysis. Some of these may be generated while considering changes over time.

*Communication and Coordination*

Many of the factors that lead to losses involve inadequate communication and coordination among components of the safety control structure. Lack of coordination and communication can lead to inconsistent actions, missing actions, and so on.

An example can be found in the collision of two aircraft in 2002 over Überlingen, a town in southern Germany in 2003. A poorly planned maintenance activity resulted in almost all the communication links in the air traffic control tower being temporarily broken. Some of the outages were known ahead, others resulted from an error during the maintenance. Planning for the loss of communication would have helped. For example, the air traffic controller on duty did not know that his aural and visual alerts about a potential collision would be inoperable during the maintenance. Contingency actions could have been taken to cope with the maintenance activity if it had been planned and management of change procedures used. The communication outage eliminated all the built-in redundancy that was designed to prevent such collisions.

지금까지 설명한 CAST 분석 프로세스는 개별 시스템 컴포넌트와 다른 컴포넌트에 대한 컨트롤에 초점을 두고 있다. 즉, 각 컨트롤러가 할당된 컨트롤 및 제약사항을 시행할 수 없었던 이유를 조사하였다.

이와 반대로 이 파트에서는 CAST에서는 컨트롤 스트럭처를 전체로서 살펴보고 컨트롤의 비효율성을 초래하는 시스템적 요소를 살펴본다. 이는 분석 중 어쩌면 가장 구조화되지 않은 부분이지만 이번 섹션에서 우리가 무엇을 찾아야 하는지 그리고 그것을 찾았을 때 역할을 어떻게 기술할 지에 대한 지침이 제공하고자 한다.

시스템적 분석 방법은 시스템의 위험한 상태를 방지하기 위해 안전 컨트롤 스트럭처 내에서 함께 작동하는 모든 컴포넌트의 동작과 상호작용에 영향을 미치는 요소에 초점을 맞추고 있다. 시스템을 개별 컴포넌트가 아닌 전체로서 살펴봄으로써 다양한 안전 컨트롤 스트럭처의 상호작용 방식에 영향을 미치는 원인 요소를 식별할 수 있다. 이러한 시스템적 요소는 왜 개별 컴포넌트가 그들의 안전 책임을 이행하지 못할 수도 있는지, 그리고, 아울러 왜 그들의 동작이 시스템의 안전 제약사항을 충족시키지 못하는지를 이해하기 위한 또 다른 방법을 제공한다. 즉, 안전 컨트롤 스트럭처는 일반적으로 하나의 컴포넌트 오작동만으로 사고로 이어지지 않도록 만들어진다. 그러나 시스템적 원인 요소는 많은 또는 모든 컴포넌트의 동작에 부정적인 영향을 미칠 수 있고 그 동작을 헛되게 할 수 있다.

이것은 사고 분석 시 스위스 치즈 모델이나 도미노 모델과 같은 이벤트 기반 모델에서 간과하는, 시스템 접근 방식의 고유한 특성이다. 모든 보호장벽이 제대로 작동하지 못하게 만드는 동시에 사고를 방지하기 위해 만들어진 모든 보호 장치와 치즈 조각에 “구멍”을 야기할 수 있는 원인 요소가 있다. 몇 가지 원인 요소에 초점을 맞추거나 하나 또는 몇 개의 컴포넌트 동작만으로 사고를 설명하려는 관점에서 벗어난다면 매우 강력한 예방 조치를 식별할 수 있는 더 큰 관점을 가질 수 있다.

다음은 고려할 수 있는 몇 가지 시스템적 요소이다. 이 목록은 모든 것을 아우르는 것은 아니며 시작점일 뿐이다.

- 의사소통 및 조정
- 안전 정보 시스템
- 안전 관리 시스템의 설계
- 안전 문화
- 시간에 따른 변경 및 변동성: 시스템 및 환경 내에서
- 기존의 분석에서 다루어지지 않은 시스템 환경에서의 내·외부 경제적 요소 및 관련 요소. 시간에 따른 변경을 고려하였을 때 이러한 것들 중 일부가 발생할 수 있다.

### 의사소통 및 조정

손실로 이어지는 많은 요소들은 안전 컨트롤 스트럭처 컴포넌트 간의 부적절한 의사소통 및 조정과 관련이 있다. 조정과 의사소통의 부족은 일관성 없는 행동, 행동 누락 등으로 이어질 수 있다.

2003년 독일 남부의 한 마을인 위버링겐(Überlingen)에서 발생한 두 대의 항공기 충돌사고를 예시로 들 수 있다. 잘못 계획된 유지보수 활동으로 인해 항공 교통 관제탑의 거의 모든 의사소통 링크가 일시적으로 끊어졌다. 일부 정전은 미리 알려져 있었지만 나머지는 유지보수 과정의 오류로 인해 발생했다. 만약 의사소통 두절에 대비한 계획이 있었다면 도움이 되었을 것이다. 예를 들어 근무 중인 항공 교통 관제사는 유지보수 과정에서 잠재적 충돌에 대한 청각적 및 시각적 경고가 작동하지 않았다는 것을 알지 못했다. 우발상황에 대한 조치를 계획하고 변경절차를 관리했다면 유지보수 활동에 대처하기 위한 조치를 취했을 수도 있다. 충돌 방지를 위해 설계되어 있는 모든 이중화가 의사소통 두절로 인해 작동하지 않았다.

Drawing the communication links as intended and what was operational during the accident can provide an important visual explanation. Figure 16 shows the communication channels that were designed into the system. Figure 17 shows those that were working at the time of the collision. This type of diagram is a powerful tool for understanding and communicating about what happened and why. The phone lines were out so that a controller at another site who saw the collision about to happen, could not get through to give a warning. When the air traffic controller who was controlling the two aircraft at the time of the collision became overloaded due to an unforeseen emergency landing, there was no way for him to contact another air traffic control facility to help him with his overload.

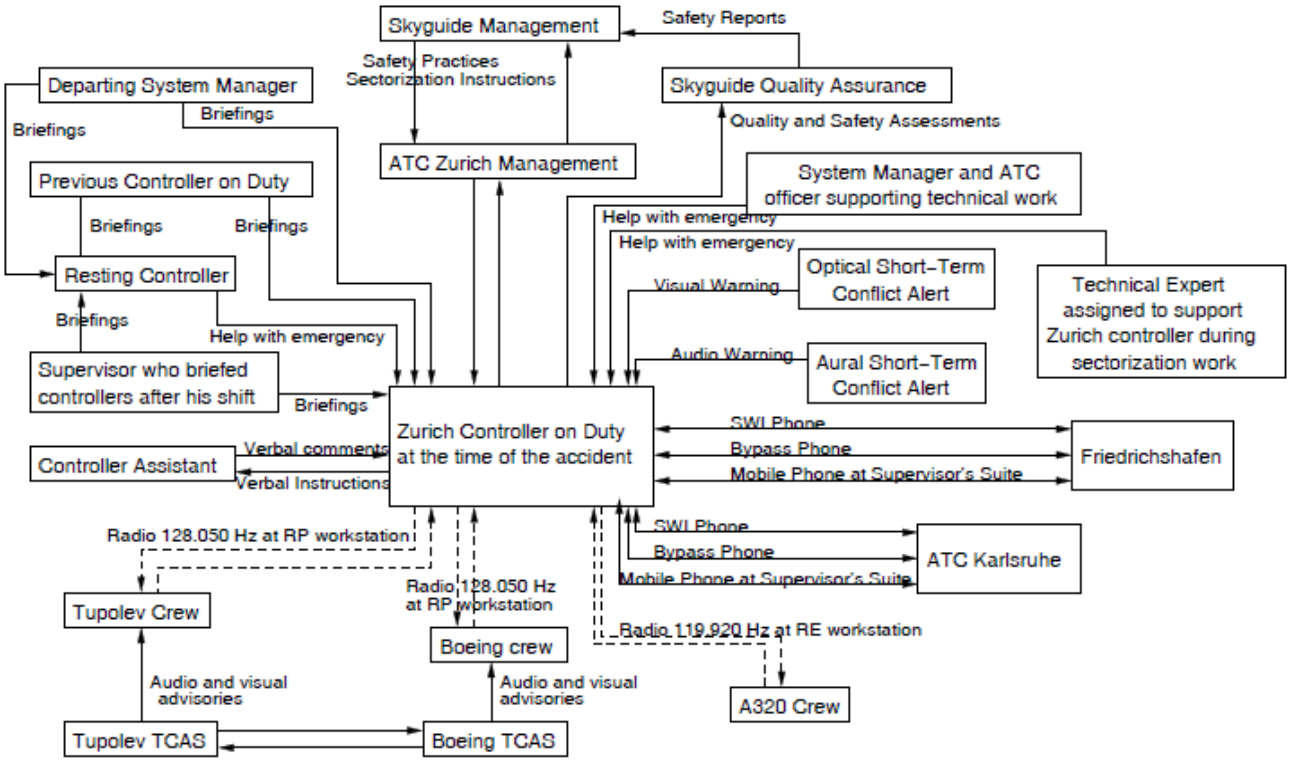



**Figure 16**: Communications links theoretically in place in the Überlingen accident

기존에 의도했던 의사소통 링크와 사고 시 실제 작동한 링크를 그림으로 그리면, 중요한 시각적 설명을 얻을 수 있다. 그림 16은 시스템에 설계된 의사소통 채널을 보여준다. 그림 17은 충돌 당시에 작동했던 의사소통 채널을 보여준다. 이러한 유형의 다이어그램은 무슨 일이 왜 일어났는지 이해하고 전달할 수 있는 강력한 도구이다. 전화가 불통이었기 때문에 곧 충돌이 일어날 것을 본 다른 사이트의 컨트롤러는 경고를 전달할 수 없었다. 충돌 당시에 두 비행기를 컨트롤하고 있던 항공 교통 관제사가 예기치 못한 비상 착륙으로 인해 과부하 상태가 되었을 때, 그가 다른 항공 교통 관제 시설에 연락하여 그의 과부하를 지원받을 방법은 없었다.

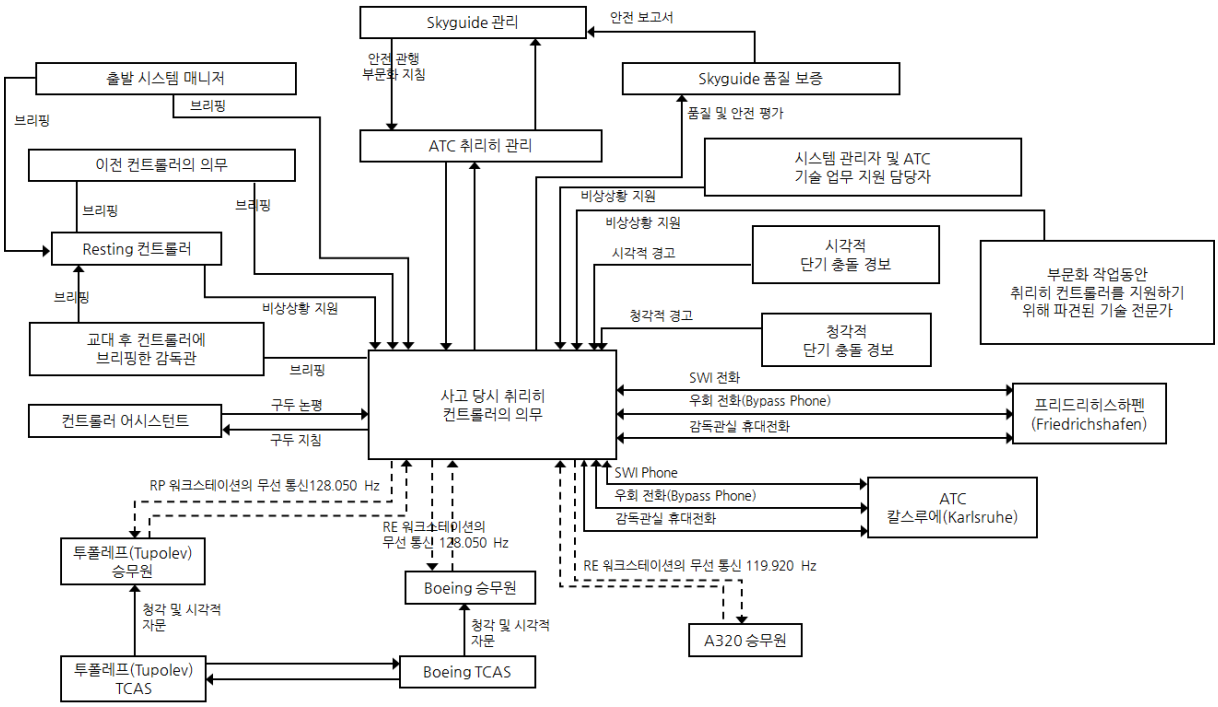



그림 16: 위버링겐(Überlingen) 사고에서의 이론적 의사소통 링크

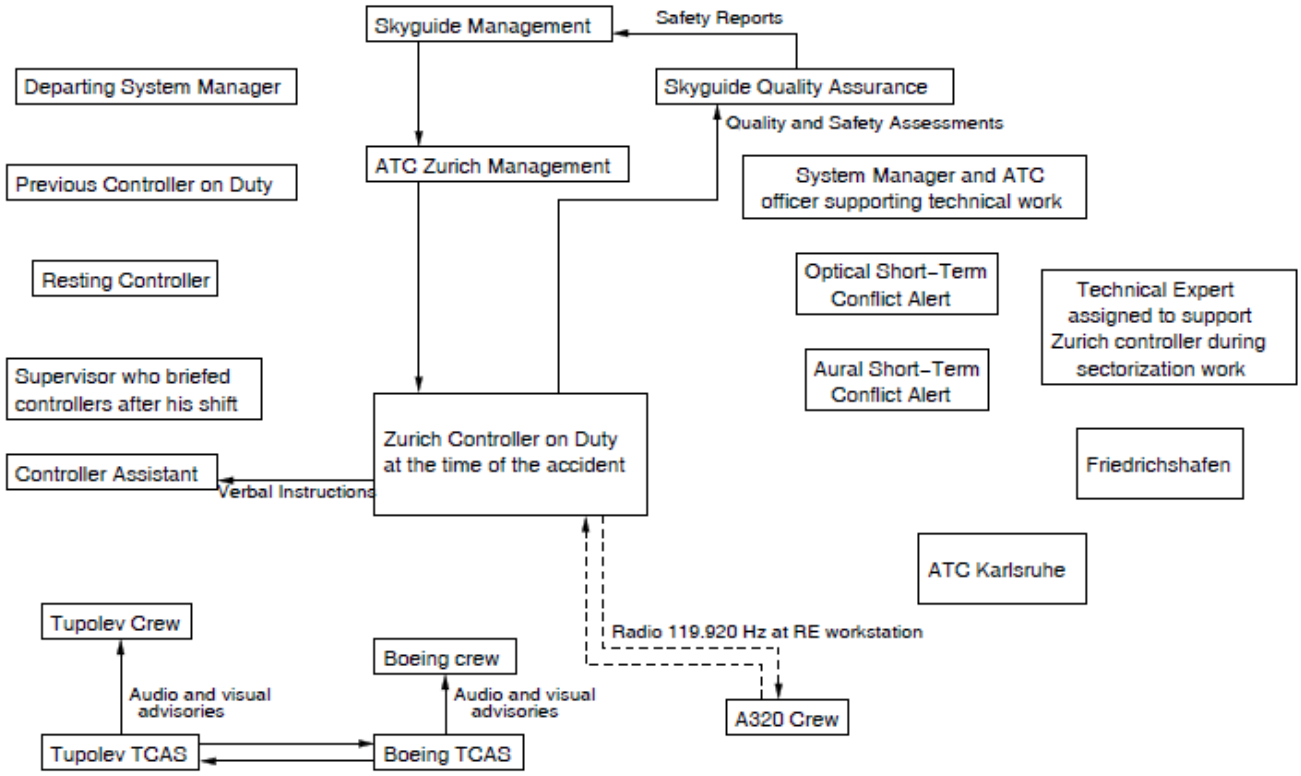



**Figure 17**: The operational communication links at the time of the accident

The communication and coordination problems in this case were confined to the time of the accident. But they can exist for a long time before. Sometimes, one controller assumes that another is handling a responsibility while the other one thinks the first is. As an example, in a Canadian water contamination incident, both the Ministry of the Environment (MOE) and the Ministry of Health (MOH) were responsible for performing some of the same oversight duties: the local MOH facility assumed that the MOE was performing this function and cut back on their own activities, but the MOE's budget had been cut, and follow-ups were not done. A common finding after an accident is that each of the responsible groups may assume another controller is performing the needed oversight when there are overlapping responsibilities. Alternatively, the two controllers may have non-overlapping responsibilities but they may provide indirectly conflicting commands.

Inadequate feedback in the safety control structure is one important type of communication that is often found to contribute to poor decision making. Other types of communication are, of course, also important. In the Shell Moerdijk accident, there were instances of ineffective communication between Shell Global Projects and Technology and Shell Moerdijk and between groups within Shell Moerdijk itself. In addition, the change to the catalyst by the manufacturer was not communicated to Shell. Did the required communication channels exist at the time of the accident? Were they fully operational or were there inhibitors to the transmission of required information?

In a friendly fire accident analyzed in Chapter 5 of *Engineering a Safer World*,[17] potential ambiguity in the responsibility for tracking friendly aircraft had been eliminated by partitioning the tracking responsibility between two different controllers. This partitioning broke down over time due to factors such as unofficial attempts to increase efficiency, with the result that neither was tracking the aircraft

[17] Nancy Leveson, *Engineering a Safer World*, MIT Press, 2012, Chapter 5.

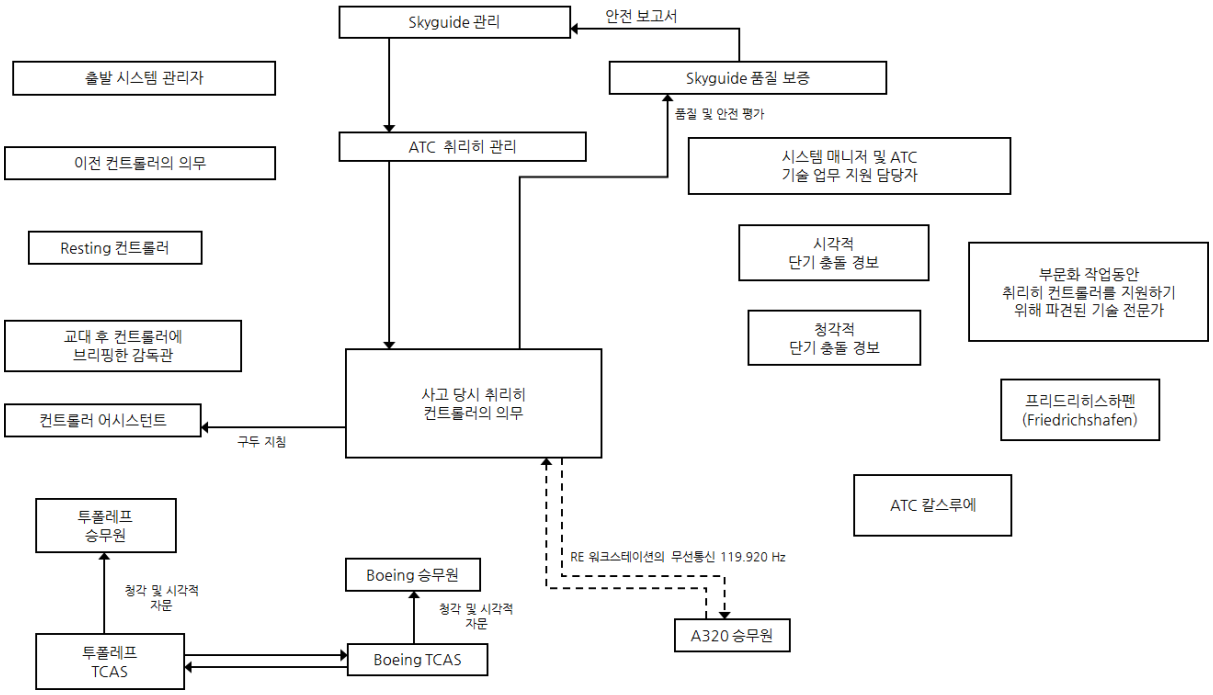



그림 17: 사고 당시의 작업 의사소통 링크

이 사례에서 의사소통과 조정 문제는 사고 당시에만 해당되었지만, 그 문제는 오래전부터 존재한 것일 수 있다. 때로는 한 컨트롤러가 다른 컨트롤러가 책임지고 있다고 여기는 반면, 다른 컨트롤러는 전자의 컨트롤러가 책임지고 있다고 생각할 수 있다. 한 예로 캐나다 수질오염 사건에서 환경부(MOE)와 보건부(MOH)는 동일한 감독 업무를 수행했다: 한 지역의 보건부 시설은 환경부가 감독 업무를 수행하고 있다고 가정하여 활동을 줄였지만 환경부의 재정이 삭감되었고 이후 후속 조치(역주: 보건부가 감독을 강화하는 것)가 이루어지지 않았다. 사고 이후에 발견되는 공통점은 책임이 그룹간 중복되어 있을 때 책임을 가진 각 그룹들이 다른 컨트롤러가 감독을 수행하고 있다고 가정할 수도 있다는 것이다. 또는 두 컨트롤러의 책임이 중복되지 않아도 간접적으로 충돌하는 명령을 제공할 수도 있다.

부적절한 피드백은 안전 컨트롤 스트럭처에서 잘못된 의사결정에 기여하는 중요한 의사소통 유형 중 하나이다. 물론 다른 유형의 의사소통도 중요하다. 쉘 뫼르딕 사고에서는, 쉘 글로벌 프로젝트 앤 테크놀로지(Shell Global Projects and Technology)와 쉘 뫼르딕간의 비효율적인 의사소통과 쉘 뫼르딕 자체 내 그룹간의 비효율적인 의사소통 사례가 있었다. 또한, 촉매제의 변경사항이 제조업체에서 쉘 뫼르딕으로 의사 전달되지 않았다. 사고 당시에 요구되는 의사소통 채널이 있었는가? 그 채널들이 완전하게 작동하고 있었는가? 요구되는 정보의 전송을 방해하는 요인이 있었는가?

*Engineering a Safer World*[17] 5장에서 분석한 아군 포격 사고에서는 아군 항공기 추적 책임에 대한 잠재적인 모호성을 제거하기 위해 추적에 대한 책임을 두 개의 서로 다른 컨트롤러가 나누어 가졌다. 이 책임의 분할은 효율성을 높이려는 비공식적인 시도와 같은 원인으로 인해 시간이 지남에 따라 실패하였으며, 그 결과, 사고 당일에는 항공기를 추적하지 못했고 격추되는 것도 추적하지 못했다. 안전 컨트롤 스트럭처 컴포넌트의 가정과 설계된 동작이 실제로 이루어졌는지 확인하기 위한 감사는 수행되지 않았다.

[17] Nancy Leveson, Engineering a Safer World, MIT Press, 2012,Chapter 5.

that was shot down on the day of the loss. No performance auditing had been done to ensure that the assumed and designed behavior of the safety control structure components was actually occurring.

After an accident, all communication links should be examined to ensure that the design allowed for the transmission of critical information. Even if the design was adequate, were the transmission channels working properly? If not, the reasons for the inadequate communication must be determined. Sometimes a communication channel involves a person who has conflicting goals with the communication of the information. In some cases, the communication links may simply have failed. In others, they may be purposely down for maintenance purposes, as in the Überlingen accident. Occasionally, communication and coordination links may have been available, but the controller did not know about them. In the friendly fire example, the links degraded and became inactive over time.

Analyzing communication requires first understanding and modeling the critical communication channels. The control structure below, created by Captain Paul Nelson in his CAST analysis of a wrong runway takeoff accident at Lexington Airport, shows dotted lines where the communication channels never existed (some involving feedback channels that were never included in the design) or were inoperable for various reasons at the time of the accident. Simply drawing the safety control structure and finding missing feedback channels in the design is a strong clue that there is a problem with the control structure design. All control loops should have feedback channels for proper decision making to occur.

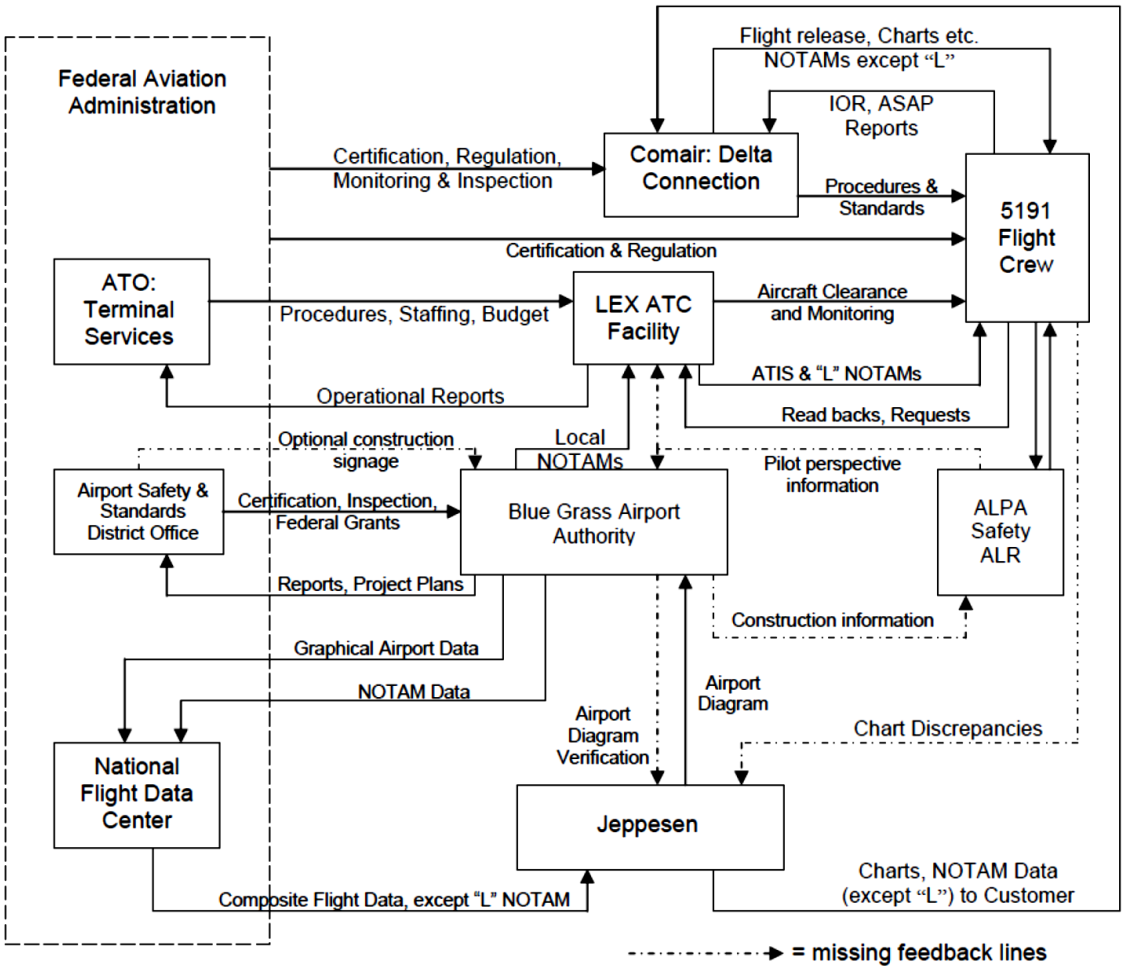



**Figure 18**: The Lexington ComAir wrong runway accident safety control structure. The control is drawn left to right instead of top to bottom. Dotted lines represent missing feedback and communication that contributed to the loss [Paul Nelson, A STAMP Analysis of the LEX Comair 5191

사고 이후에 의사소통 링크를 조사하여 중요한 정보가 전송될 수 있도록 설계되어 있었는지를 조사해야 한다. 설계가 적절했다 할지라도 전송 채널이 제대로 작동하였는가? 그렇지 않다면 부적절한 의사소통의 이유를 반드시 파악해야 한다. 의사소통 채널에는 종종 정보 전달과 상충되는 목표를 가진 사람이 포함되어 있다. 어떤 경우에는 단순히 의사소통 링크가 실패했을 수도 있다. 또한 위버링겐 사고에서처럼 유지보수 목적으로 의도적으로 다운되었을 수 있다. 때로는 의사소통 및 조정 링크를 사용할 수 있지만 컨트롤러가 이 링크에 대해 알지 못한 경우도 있다. 아군 포격 사례에서 의사소통 링크는 시간이 지남에 따라 기능이 저하되었고 비활성화 되었다.

의사소통을 분석하려면 우선 중요한 의사소통 채널을 이해하고 모델링해야 한다. 아래 컨트롤 스트럭처는 폴 넬슨(Paul Nelson) 기장이 작성한 것으로 렉싱턴(Lexington) 공항에서의 잘못된 활주로 이륙 사고에 대한 그의 CAST 분석에서 발췌한 것이다. 이 컨트롤 스트럭처에서의 점선은 의사소통 채널이 존재하지 않았거나(설계에 포함되지 않은 피드백 채널이 일부 포함됨) 사고 당시 여러 가지 이유로 작동할 수 없었던 의사소통 채널을 의미한다. 간단하게 안전 컨트롤 스트럭처 그림을 그려서 설계에서 누락된 피드백 채널을 찾는 것만으로도 컨트롤 스트럭처 설계에 문제가 있다는 강력한 단서가 된다. 모든 컨트롤 루프는 적절한 의사결정을 위한 피드백 채널을 가져야 한다.

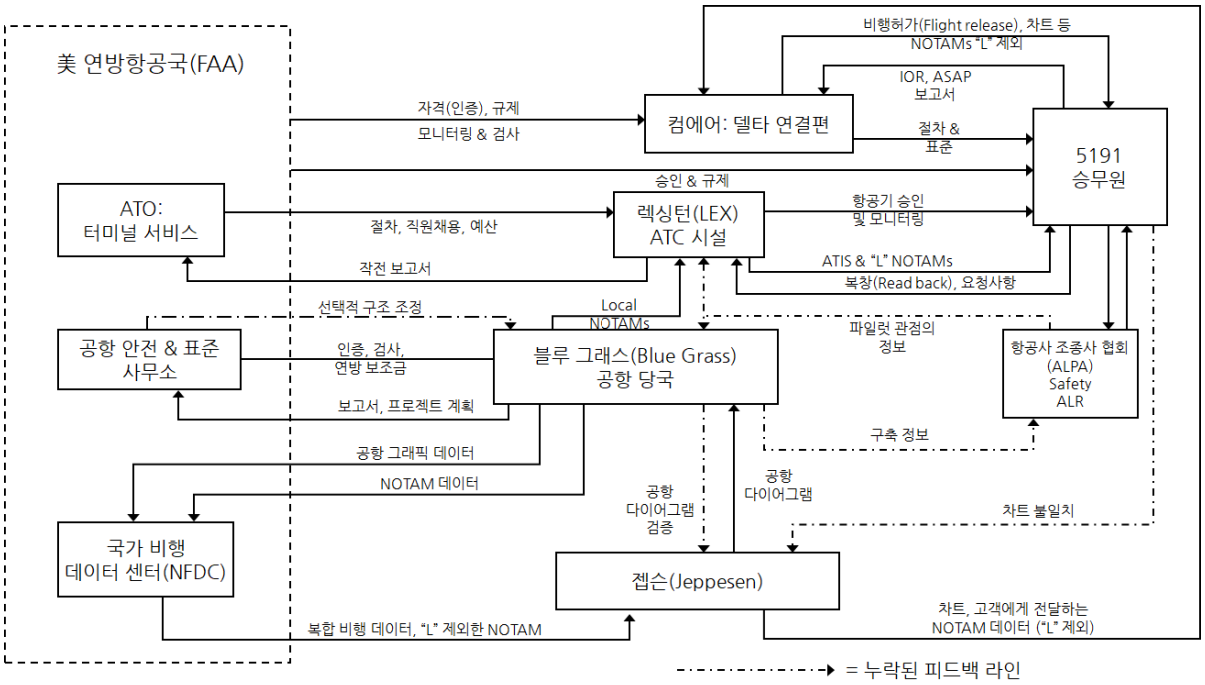



그림 18: 렉싱턴 공항에서의 컴에어 항공의 잘못된 활주로 사고에 대한 안전 컨트롤 스트럭처. 컨트롤은 위에서 아래가 아니라 왼쪽에서 오른쪽으로 그려짐. 점선은 손실에 기여한 누락된 피드백 및 의사소통을 나타냄. [폴 넬슨, A STAMP Analysis of the LEX Comair 5191 Accident, Master's Thesis, Lund University, June 2008. 이 논문의 링크는 부록 A 참조]

Accident, Master's Thesis, Lund University, June 2008. A link to this thesis is provided in Appendix A.]

Another common type of communication breakdown, described earlier, can occur in the problem-reporting channels. In many accidents, the investigators find that the problems were identified in time to prevent the loss, but the required problem-reporting channels were not used, often because they were unusable.

## Safety information system

In a study of the safety information systems of various companies, Kjellan found that the quality of the safety information system was the second most important factor in discriminating between companies with high and low accident rates [Kjellan 1982].[18] Uses for a safety information system include storing and passing on information about hazards, detecting trends and deviations that portend an accident, evaluating the effectiveness of safety controls and standards, comparing models and risk assessments with actual behavior, identifying and controlling hazards to improve designs and standards, etc. Accident investigations should include an examination of the organization's safety information system (SIS).

The Shell Moerdijk accident report does not provide any information about the Shell or Shell Moerdijk SIS, but it does describe many instances of deficiencies that could have been prevented with a well-designed SIS, such as not learning from incidents and previous maintenance stops, not identifying flaws in previous hazard and risk assessments when contrary evidence arose, etc. The accident report also notes that important information was lost between the design of the unit and the ultimate operations management of the unit. The report says that "A discrepancy therefore occurred between the available information during the design phase and the operations management that was ultimately conducted." A well-designed safety information system should be able to prevent these types of problems.

Just having a safety information system does not guarantee that it will be useful or used. Data may be distorted by the way it is collected. Common problems are filtering, suppression, and unreliability. Data collected in accident and incident reports tend to focus on proximal events and actors, and not on the systemic factors involved such as management problems or organizational deficiencies. Limited categories of conditions may be identified, especially when checklists are used. It is difficult to obtain comparable data from multiple sources in an unbiased and systematic manner.

Data collection tends to be more useful for events that are similar to those that have occurred in the past than for events in new types of systems where past experience about hazards and causal factors is more limited. Software errors and computer problems are often omitted or inadequately described in incident reports because of lack of knowledge, lack of accepted and consistent categorizations for such errors, or simply discounting them as a causal factor. CAST can be used to encourage the inclusion of systemic factors in safety information systems.

Some common deficiencies include not recording the information necessary to detect trends, changes and other precursors to an accident; to evaluate the effectiveness of the controls used to prevent accidents; to compare risk assessments of those in the industry with actual behavior; and to learn from events and improve their safety management practices.

Simply collecting the information, of course, is not enough. Problems may arise from the difficulty in consolidating a large mass of data into a form useful for learning. While with digital technology today it

[18] The highest-ranking factor was top-level management concern about safety. Urban Kjellan, An evaluation of safety information systems at six medium-sized and large firms, *Journal of Occupational Accidents*, 3:273-288, 1982.

앞서 설명한 의사소통 고장의 또 다른 전형적인 유형은 문제 보고 채널에서 발생할 수 있다. 많은 사고에서 조사관들은, 손실을 막기 위해 문제가 제때 식별되었지만 문제 보고 채널을 사용할 수 없어서 사용하지 않았다는 것을 발견하였다.

### 안전 정보 시스템(Safety information system)

킬랜(Kjellan)은 여러 회사의 안전 정보 시스템에 대한 연구를 통해 사고율이 높은 회사와 낮은 회사를 구별하는 데 안전 정보 시스템의 품질이 두 번째로 중요한 요소라는 것을 발견했다[Kjellan 1982].[18] 안전 정보 시스템의 사용에는 위험 정보에 대한 저장 및 전달, 사고의 전조가 되는 경향 및 일탈행위의 탐지, 안전 컨트롤 및 표준의 효과 평가, 모델 및 리스크 평가를 실제 동작과 비교, 설계 및 표준 개선을 위한 위험 식별 및 통제 등이 포함된다. 사고 조사에는 조직의 안전 정보 시스템(SIS)에 대한 조사가 포함되어야 한다.

쉘 뫼르딕 사고 보고서에는 쉘 또는 쉘 뫼르딕 안전 정보 시스템에 대한 정보는 제공되지 않지만, 잘 설계된 안전 정보 시스템이 있었다면 예방할 수도 있었던 유지보수 중단과 같은 결함 사례가 많이 제시되어 있다. 예를 들면, 이전의 사건 및 유지보수 중단이 발생했었음에도 그로부터 배우지 않은 것, 상충되는 증거가 발견되었음에도 이전의 위험 및 리스크 평가에서의 결함을 찾아내지 않은 것 등이다. 사고 보고서는 또한 유닛의 설계와 최종의 유닛 운영 관리 간의 중요한 정보가 손실되었다고 명시하고 있다. 보고서에 따르면 “그로 인해 설계 단계에서 가용한 정보와 최종적으로 이행된 운영 관리 간에 불일치가 발생했다”고 하였다. 잘 설계된 안전 정보 시스템은 이러한 유형의 문제를 방지할 수 있어야 한다.

안전 정보 시스템을 갖춘다고 해서 그 시스템이 유용하다거나 활용할 수 있음을 보장하는 것은 아니다. 데이터는 수집되는 방식에 따라 왜곡될 수 있다. 흔히 발생하는 문제는 필터링, 은폐(suppression), 신뢰성 부재(unreliability)이다. 사고 및 사건 보고서에서 수집된 데이터는 관리의 문제나 조직적 결함과 같은 시스템적 요소가 아닌 근접한(proximal) 이벤트 및 행위자에 초점을 맞추는 경향이 있다. 데이터가 특정한 조건의 카테고리로 제한되어 버릴 수도 있는데, 특히 체크리스트를 사용하면 그렇다. 여러 출처로부터 편파적이지 않고 체계적인 방식으로 비교 가능한 데이터를 수집하는 것은 어렵다.

데이터 수집은, 위험과 원인 요소에 대한 과거 경험이 제한적인 새로운 유형의 시스템에서 발생한 이벤트 보다는, 과거에 일어난 이벤트와 비슷한 이벤트에 대해 더 유용한 경향이 있다. 소프트웨어 오류와 컴퓨터의 문제는 지식의 부족, 오류에 대한 인정되고 일관된 분류 체계의 부족, 또는 단순히 이들을 원인 요소로는 가치가 없다고 여기는 때문에, 종종 사건 보고서에서 생략되거나 부적절하게 설명된다. CAST는 안전 정보 시스템에 시스템적 요소를 포함하도록 독려하는 데 사용될 수 있다.

몇 가지 공통된 결함으로 다음의 정보를 기록하지 않는 것이 있다; 사고의 트렌드, 변화 및 다른 전조(precursor)를 탐지하는 데 필요한 정보; 사고 방지에 사용되는 컨트롤의 효과를 평가하는데 필요한 정보; 리스크 평가와 산업계에서의 실제 동작을 비교하기 위해 필요한 정보; 이벤트로부터 배우고 안전 관리 관행을 개선하는데 필요한 정보를 기록하지 않는 것 등이 있다.

물론 단순히 정보를 수집하는 것만으로는 충분하지 않다. 많은 양의 데이터를 학습에 유용한 형태로 통합하는 데에는 어려움이 있을 수 있다. 오늘날의 디지털 기술로 대규모의 데이터 수집 채널을 쉽게

[18] 첫 번째 중요한 요소는 최상위 경영진의 안전에 대한 우려이다. Urban Kjellen, An evaluation of safety information systems at six medium-sized and large firms, *Journal of Occupational Accidents*, 3:273-288, 1982.

is easy to design large scale data collection channels, finding the time and manpower to analyze all the data that results may be difficult or impractical. As a result, the safety information system may contain only summary statistical data that can be easily processed by a computer but not the information about trends and changes over time that is needed to learn from events before major losses occur. Airlines today are particularly suffering from this type of data overload due to large-scale automated information collection.

Another deficiency of many safety information systems lies in the retrieval and dissemination mechanisms. Information—which is not the same as data—may not be presented in a form that people can learn from, apply to their daily operations, and use throughout the system life cycle. Updating may not occur in a timely manner: Accidents have resulted from changes during operations or due to insufficient updates to the hazard analyses when engineering modifications were made. The information may not be tailored to the needs and cognitive styles of the users or not integrated into the environment in which safety-related decisions are made and therefore may be hard to use.

The safety information system must also exist within a safety management system that can use and benefit from the information provided. Simply having information stored in a safety information system does not mean that companies have the structures and processes needed to benefit from it.

When conducting an accident investigation, the safety information system and any possible impact on the events needs to be examined. Was the information needed to prevent the loss not collected or stored? Was it lost in the collection or analysis process? Was it available and easily retrieved in the daily activities of controllers?

## Design of the safety management system

The safety management system (SMS) is theoretically the same as the safety control structure used in CAST analyses. The more general term "safety control structure" is used here as some industries define an SMS that excludes important controls necessary to prevent accidents.

There is no single correct design for the safety control structure: Alternative safety control structures can be effective with responsibilities distributed in different ways. The culture of the industry and the organization will play a role in what is practical and effective. There are some general design principles, however, that are necessary for any safety control structure to be effective,[19] and these can be used to evaluate an organization's safety management system after an accident. In general, the necessary safety constraints on organizational behavior should be reflected in the design of the safety control structure: Is the assignment of responsibility, authority, and accountability for safety to the controllers adequate to prevent hazards and accidents? A list of general responsibilities for management, development and operations that need to be assigned is included in Appendix D.

The accident investigation should evaluate the official design of the safety control structure as well as how it actually operated at the time of the loss. Were performance or other types of audits used to ensure that it was working effectively? Previous minor incidents may be clues that something is amiss and should have been used to identify problems before a major loss. Were near-miss and incident reporting systems used to identify flaws in the operation of the safety control structure or simply to assign blame to operators?

Clues will be available during the investigation that will provide guidance on where to look. For example, the Shell Moerdijk official accident report, which did not document or evaluate Shell's safety management system, notes that unsafe situations were overlooked, internal procedures were not properly followed, lessons were not learned from previous incidents, incorrect assumptions about basic

[19] See Leveson, *Engineering a Safer World, 2012* and Chapter 7 (Designing and Effective Safety Management System) in Leveson and Thomas, *STPA Handbook*, 2018.

설계할 수는 있지만 모든 결과 데이터를 분석하기 위한 시간과 인력을 찾는 것은 어렵거나 비현실적일 수 있다. 그 결과 안전 정보 시스템은 컴퓨터로 쉽게 처리할 수 있는 요약 통계 데이터만 제공하고 중대한 손실이 발생하기 전에 이벤트로부터 학습하기 위해 필요한 트렌드 및 시간에 따른 변화에 대한 정보는 제공하지 않을 수 있다. 오늘날의 항공사들은 대규모 자동 정보 수집에 따른 이러한 유형의 데이터 과부하로 어려움을 겪고 있다.

많은 안전 정보 시스템의 또 다른 결함은 검색(retrieval) 및 보급(dissemination) 메커니즘에 있다. 정보(데이터와 다른 것임)가 사람들이 배울 수 있고 일상 업무에 적용할 수 있으며 시스템 수명 주기 전반에 걸쳐 사용할 수 있는 형태로 제공되지 않을 수 있다. 업데이트가 적시에 수행되지 않을 수도 있다: 사고는 운영 중의 변경 또는 수정 작업을 하는 과정에서 위험 분석에 대한 업데이트가 불충분했기 때문에 발생한다. 정보가 사용자의 요구사항과 인지 유형에 맞게 테일러링되지 않거나 안전 관련 결정이 내려지는 환경에 통합되지 않아 사용하기가 어려울 수 있다.

안전 정보 시스템(SIS)은 제공된 정보를 활용할 수 있는 안전 관리 시스템(SMS) 내에 있어야 한다. 단순히 안전 정보 시스템에 정보를 저장하는 것이 기업이 정보를 활용하는 데 필요한 구조와 프로세스를 가지고 있다는 것을 의미하지는 않는다.

사고 조사를 수행할 때에는 안전 정보 시스템과 이벤트에 미칠 수 있는 모든 영향을 조사해야 한다. 손실을 막기 위해 필요한 정보가 수집되거나 저장되지 않았는가? 정보 수집이나 분석 과정에서 정보 손실이 있었는가? 정보가 컨트롤러의 일상적인 활동에서 사용 가능하고 쉽게 조회할 수 있는가?

### 안전 관리 시스템의 설계(Design of the safety management system)

안전 관리 시스템(SMS)은 CAST 분석에 사용된 안전 컨트롤 스트럭처와 이론적으로 동일하다. 일부 산업에서는 SMS를 정의할 때, 사고 방지에 필요한 중요 컨트롤을 포함하지 않기 때문에, 여기에서는 더 일반적인 용어인 “안전 컨트롤 스트럭처”를 사용한다.

안전 컨트롤 스트럭처의 올바른 설계는 한 가지가 아니다. 다양한 방식으로 책임을 분산시키는 효과적인 안전 컨트롤 스트럭처가 다수 있을 수 있다. 산업과 조직에서의 문화는 그 산업 및 조직이 실용적이고 효과적으로 기능하는 데 중요한 역할을 할 것이다. 그러나 안전 컨트롤 스트럭처가 효과적이기 위해서는 몇 가지 일반적인 설계 원칙이 있는데[19] 이는 사고 발생 후에 조직의 안전 관리 시스템을 평가하는 데 사용될 수 있다. 일반적으로 조직 행동에 필요한 안전 제약사항은 안전 컨트롤 스트럭처의 설계에 반영되어야 한다: 안전에 대한 책임, 권한 및 의무의 할당이 위험과 사고를 방지하는 데 적절한가? 할당해야 하는 관리, 개발 및 운영의 일반적인 책임에 대한 목록은 부록 D에 나와 있다.

사고 조사에서는 안전 컨트롤 스트럭처의 공식적인 설계뿐만 아니라 손실 당시의 실제 동작 방식을 평가해야 한다. 안전 컨트롤 스트럭처가 효과적인지 확인하기 위해 성능 또는 다른 유형의 감사가 이루어졌는가? 이전에 발생한 마이너한 사건은 무언가 잘못되었다는 단서일 수 있으며 그 사건은 중대한 손실이 발생하기 전에 문제를 식별하기 위해 사용되어야 한다. 니어 미스 및 사건 보고 시스템이 안전 컨트롤 스트럭처의 운영상 결함을 식별하거나 단순히 운영자에게 책임을 부여하기 위해 사용되었는가?

조사 과정에서, 어디를 살펴봐야 하는지에 대한 지침을 제공하는 단서를 찾을 수 있을 것이다. 예를 들면, 쉘의 안전 관리 시스템을 문서화하거나 평가하지 않은 쉘 뫼르딕의 공식 사고 보고서는, 안전하지

[19] Leveson, Engineering a Safer World 2012 and Chapter 7 (Designing and Effective Safety Management System) in Leveson and Thomas, STPA Handbook, 2018 참조.

chemical reactions were not re-evaluated after evidence surfaced that they were incorrect, changes were not managed and controlled, inadequate hazard analysis and risk assessment procedures were used, recommendations from previous incidents and accidents were never implemented, and oversight of critical activities was missing. Were responsibilities assigned for performing and overseeing these activities? What types of audits or inspections were used to identify these types of poor practices? Why were they not identified and corrected before the accident?

Oversight of a company's safety management system (SMS) usually lies in the responsibilities of government or professional regulatory agencies or organizations. At Shell Moerdijk, for example, the Dutch Regulatory Authorities have the responsibility to check whether the company has a safety management system in place, whether the systems and procedures incorporated in that system are appropriate, and whether the company actually applies these systems and procedures. They did not notice or did not react to Shell not acting in accordance with its own SMS. As just some examples, changes and upgrades to the plant were not consistently subjected to risk analyses, which violated the Shell SMS requirements, but this deficiency was not noted by the regulators nor required to be fixed. Changes were not adequately evaluated for safety. Requirements for expertise and training in performing startups were not enforced.

In fact, the regulators were unanimous in their positive appraisal of the Shell Moerdijk SMS. Government inspections and supervision are partly determined by the judged quality of the SMS, so oversight activities were limited for Shell Moerdijk. The Dutch Regulatory Authorities did not have adequate resources (a common problem) and thus allocated them based on perceived risk. They only perform "system-oriented supervision," that is, if the right systems are in place, then the authorities do not look further at the actual activities in the plant. The official accident report notes, however, that even under this type of limited supervision, it was possible for the inspectors to observe that changes and upgrades to the plant were not consistently subjected to risk analyses and that the safety management system did not indeed function well.

In the Shell Moerdijk accident, there had been two previous incidents involving the same catalyst, neither of which seemed to generate concerns or questions about the design of the plant, the risk assessments that were performed, or the creation of the start-up work instructions. The information about the incidents may not have been effectively stored by Shell (and thus stemmed from a deficiency in the safety information system), but more likely it simply was not used due to deficiencies in the operation of the company's safety management system. Asking appropriate questions during the investigation could have identified the source of these problems.

## Safety culture

Acceptable safety information systems and safety management system structures can both be defeated by safety culture problems. In fact, the safety culture in an organization or industry impacts the behavior of every component in the safety control structure.

Edgar Shein, considered to be the "father of organizational culture," defined safety culture as "*the values and assumptions in the industry and/or organization used to make safety-related decisions*"[20] Figure 19 shows Shein's three levels of organizational culture and, more specifically, safety culture.

[20] Edgar Shein, *Organizational Culture and Leadership*, San Francisco: Jossey Bass, 2004

않은 상황이 간과되었던 것, 내부 절차가 제대로 지켜지지 않았던 것, 이전 사건에서 교훈을 얻지 못한 것, 기본적인 화학 반응에 대한 가정이 잘못되었다는 증거가 드러난 후에도 그 가정이 재평가되지 않은 것, 변경사항들이 관리 및 컨트롤되지 않았던 것, 부적절한 위험 분석 및 리스크 평가 절차가 사용된 것, 이전 사건과 사고로부터의 권고사항이 이행되지 않은 것, 크리티컬한 활동에 대한 감독이 누락된 것을 명시하고 있다. 이러한 활동들을 수행하고 감독할 책임이 할당되었는가? 이러한 유형의 잘못된 사례를 식별하기 위해 어떤 유형의 감사 또는 검사가 사용되었는가? 왜 사고 발생 전에 식별 및 수정되지 않았는가?

회사의 안전 관리 시스템(SMS)에 대한 감독은 일반적으로 정부, 전문 규제기관 또는 조직의 책임이다. 예를 들어 쉘 뫼르딕에서 네덜란드 규제 당국은 회사가 안전 관리 시스템을 갖추었는지, 그 시스템 및 시스템에 통합된 절차가 적절한지, 회사가 실제로 이러한 시스템과 절차를 적용했는지를 확인할 책임이 있다. 그들은 쉘이 SMS에 따라 행동하지 않은 것을 알아차리지 못했거나 대응하지 않았다. 일부 사례와 마찬가지로 플랜트의 변경사항 및 업그레이드에 대한 위험 분석을 지속적으로 수행하지 않아 쉘 SMS 요구사항을 위반하였지만 규제 기관은 이 문제를 지적하지 않았고 따라서 수정될 필요도 없었다. 변경사항에 대한 안전성 평가가 제대로 이루어지지 않았다. 기동 작업 수행에 대한 전문성과 훈련 요구사항은 이행되지 않았다.

실제로 규제기관은 쉘 뫼르딕의 SMS에 대해 만장일치로 긍정적으로 평가하였다. 정부의 검사와 감독은 SMS 품질의 평가결과에 의해 부분적으로 결정되므로 쉘 뫼르딕에 대한 감독 활동이 제한적으로 수행되었다. 네덜란드 규제 당국은 자원의 부족(공통적인 문제임)으로 인해 파악된 리스크의 정도에 따라 자원을 할당하였다. 그들은 "시스템 중심의 감독(system-oriented supervision)"만을 수행한다. 즉, 제대로 된 시스템이 마련되면 규제 당국은 더 이상 플랜트의 실제 활동을 보지 않는다. 그러나 공식 사고 보고서에서는 이러한 제한된 감독을 하였을지라도 기업이 플랜트의 변경 및 업그레이드에 대해 지속적으로 리스크 분석을 수행하지 않았으며, 안전 관리 시스템이 실제로 잘 작동하지 않는다는 것을 검사관이 관찰할 수 있었다고 지적했다.

쉘 뫼르딕 사고에서 동일한 촉매제와 관련된 이전의 두 번의 사건이 있었는데 두 사건 모두 플랜트 설계, 수행된 리스크 평가 또는 기동 작업 지침 작성에 대한 우려나 질문을 제기하지 않는 듯 했다. 쉘이 사건에 대한 정보를 효과적으로 저장하지 않았을 수도 있지만(안전 정보 시스템의 결점으로 인한 것) 기업의 안전 관리 시스템의 운영상 문제로 인해 사용되지 않았을 가능성이 더 높다. 조사 과정에서 적절한 질문을 했다면 이와 같은 문제의 원인을 파악할 수 있었을 것이다.

### 안전 문화(Safety culture)

수용 가능한 안전 정보 시스템 및 안전 관리 시스템의 구조는 안전 문화의 문제로 인해 모두 무너질 수 있다. 실제로 조직이나 산업에서의 안전 문화는 안전 컨트롤 스트럭처의 모든 컴포넌트 동작에 영향을 미친다.

"조직 문화의 아버지"라 불리는 에드거 샤인(Edgar Shein)은 안전 문화를 "안전 관련 결정을 내리는데 사용되는 산업 및/또는 조직의 가치와 가정"[20]이라고 정의했다. 그림 19는 샤인의 세 단계의 조직 문화, 특히 안전 문화를 보여준다.

[20] Edgar Shein, *Organizational Culture and Leadership*, San Francisco: Jossey Bass, 2004

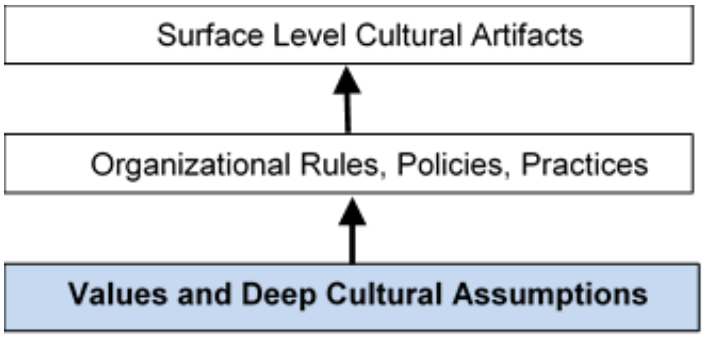



**Figure 19**: Shein's model of organizational culture

The essence of culture is the lowest-level set of values and deep cultural assumptions that underlie decision-making and the higher-level cultural artifacts in an organization or industry. The middle and top levels are not the culture; they merely reflect the organizational culture.

There is always a safety culture. The important question is how the existing safety culture impacts accident rates. Some aspects of safety culture that you might look for when investigating an accident are:

- Culture of Risk Acceptance: This culture is based on the assumptions that accidents are inevitable and that nothing much can be done to prevent them beyond exhorting everyone to be careful. Accidents are considered to be the price of productivity. Often this assumption is accompanied by the belief that everyone should be responsible for safety—their own and others—and that accidents result from a lack of responsible behavior on the part of individuals. The belief is prevalent that if only everyone would act responsibly and safely, accidents would be reduced or even eliminated.
- Culture of Denial: In a culture of denial, risk assessment is often unrealistically low, with credible risks and warnings being dismissed without appropriate investigation: Management only wants to hear good news so that is what they are told. The focus is on showing the system is acceptably safe, not on identifying the ways it might be unsafe. The use of "safety cases" rather than hazard analyses, is common.
- Culture of Compliance: The focus here is on complying with government regulations. The underlying cultural belief is that complying with regulations will lead to acceptable results. Because regulatory agencies tend to focus on certifying that a final product or service is safe, assurance of the safety of completed or existing designs is emphasized rather than building safety into the design during development. Often extensive "safety case" arguments are produced for managers or regulators with little or no impact on the actual product or product design effort. In addition, the bulk of the safety efforts may involve complying with standards and the requests of regulators instead of proactively taking steps to improve safety because it is a basic value in the organization. Even if employees fix immediately what is found to be lacking by government inspectors, did they aggressively search for problems internally without being prompted by a regulatory agency?
- Paperwork Culture: This culture rests on the belief that producing lots of documentation and analysis paperwork leads to safe products and services. Piles of paper analyses are produced but they have little real impact on design and operations. The bulk of the safety-related paperwork may be produced by a group that is independent from and has little interaction with those who

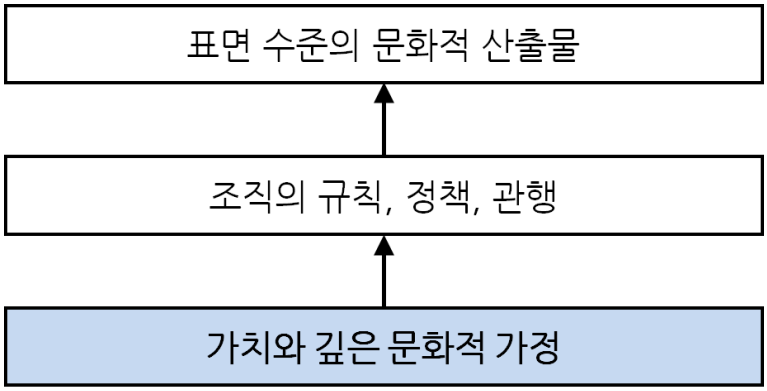



그림 19 : 샤인(Shein)의 조직 문화 모델

문화의 본질은 가장 낮은 단계에 있는 가치와 깊은 문화적 가정이며, 조직이나 산업에서 의사 결정 및 그 위의 단계들에 있는 문화적 산출물의 기초가 된다. 중간 및 제일 높은 단계는 문화가 아니다; 그것은 단지 조직 문화를 반영할 뿐이다.

안전 문화는 항상 존재한다. 중요한 질문은 기존의 안전 문화가 사고율에 어떤 영향을 미치는가이다. 사고를 조사할 때 발견할 수 있는 안전 문화의 일부는 다음과 같다:

- 리스크 수용 문화(Culture of Risk Acceptance): 이 문화는, 사고는 불가피하므로 사고 방지를 위해서는 모든 사람들이 조심하도록 적극 권유하는 것 이상으로는 할 수 있는 일이 없다는 가정을 기반으로 한다. 사고는 생산성에 따르는 대가로 간주된다. 종종 이 가정은 모든 사람이 안전에 —자신의 안전 및 타인의 안전—책임을 져야 하며, 사고는 개인의 책임 있는 행동이 부족하여 발생한다는 믿음을 동반한다. 이 문화에서는 모든 사람이 책임감 있고 안전하게 행동하기만 한다면 사고는 줄어들 것이라는 믿음이 일반적이다.
- 부정의 문화(culture of denial): 부정의 문화에서는 리스크 평가(assessment)가 비현실적으로 낮은 경우가 많으며 신뢰할만한 리스크 및 경고가 적절한 조사 없이 무시된다: 관리자는 좋은 소식만을 듣고 싶어 하며 그렇기 때문에 좋은 소식만을 듣는다. 시스템이 안전하지 않을 수 있는 경우를 식별하는 것이 아니라 시스템이 수용 가능한 수준으로 안전하다는 것을 보여주는 데 중점을 둔다. 위험 분석보다 "세이프티 케이스(safety cases)"를 활용하는 것이 일반적이다.
- 규정 준수 문화(Culture of Compliance): 여기서는 정부 규제를 준수하는 데 중점을 둔다. 규제를 따르는 것이 수용 가능한 결과를 가져온다는 근본적인 문화적 신념을 가진다. 규제기관은 최종 제품이나 서비스의 안전에 대한 자격 부여에 초점을 두는 경향이 있기 때문에 개발 과정에서 설계에 안전성을 구축하기보다는 완성된 설계 또는 기존 설계의 안전성 보장을 강조한다. 관리자나 규제기관이 실제 제품이나 프로세스 안전에 거의 또는 전혀 영향을 미치지 않는 "세이프티 케이스(safety case)"에 대한 논의만 방대하게 제기하는 경우가 종종 발생한다. 또한 표준과 요구사항을 준수하는 것은 조직의 기본 가치이기 때문에 안전을 위한 노력의 대부분이 안전 개선을 위한 사전 조치보다는 표준과 규제기관의 요구사항 준수에 사용될 수 있다. 정부 감사관이 부족하다고 지적한 것을 직원들이 즉시 고친다고 할지라도, 직원들이 규제기관의 지시 없이도 내부적인 문제를 적극적으로 조사하겠는가?
- 문서 작업(Paperwork) 문화: 이 문화는 많은 문서의 작성 및 분석이 안전한 제품과 서비스로 이어질 것이라는 믿음에 기초한다. 많은 문서 분석이 이루어져도 대부분 설계 및 운영에 거의 영향을 미치지 않는다. 안전-관련 문서 작업의 대부분은, 제품을 설계 및 운영하거나 프로세스를

are designing and operating the products, implementing the processes, or providing the services. The paperwork sits in files, assuring everyone that the system is safe.

- Culture of "Swagger": Safety is for sissies. Real men thrive on risk. The problem here with respect to preventing accidents is, of course, obvious.

The safety culture in any organization is set by the top management. A sincere commitment by management to safety is often cited as the most important factor in achieving it. Employees need to feel that they will be supported if they exhibit a reasonable concern for safety in their work and if they put safety ahead of other goals such as schedule and cost. Often, concern for safety is merely lip-service and sloganeering. Employees take their cues from actions, not from empty words.

Analysis of the safety culture during an accident investigation should start with an evaluation of the company's documented safety philosophy and safety policy. If these do not exist, then there clearly is a problem. After a serious safety problem was found in a medical device, I was asked by the company to come in and investigate what happened. I had told them previously that they needed a written safety policy, but they had never produced one. After the safety problems in their products, I asked why and was told that it should have been obvious to the employees that the devices they were designing and selling were safety-critical and therefore a policy was not needed. At the same time, there were lots of written policies and rules about other product properties. In addition, they said that their lawyers had advised them not to create a safety policy because it was an admission that their product was potentially hazardous. The hazardous nature of the product was obvious and the lack of a safety policy would not have fooled anyone into thinking that there were no hazards associated with it. It simply made the company look negligent. Shortly after the adverse events that I was consulted about, the company went bankrupt and ceased to exist.

The safety philosophy is a short, written statement of the relationship that management desires between safety and other organizational goals. Some examples of general principles that might be part of the Safety Philosophy statement:

1. All injuries and accidents are preventable.
2. Safety and productivity go hand in hand. Improving safety management leads to improving other quality and performance factors. Maximum business performance requires safety.
3. Safety has to be built into a product or the design of a service. Adding it later will be less effective and more expensive. After-the-fact assurance cannot guarantee a safe design where safety is not already present. It is better to build safety in than try to ensure it after the fact.
4. The goal of accident/incident causality analysis is to determine why the loss (or near loss) occurred so that appropriate changes can be made rather than to find someone or something to blame.
5. Incidents and accidents are an important window into systems that are not operating safely and should trigger comprehensive causal analysis and improvement actions.
6. Safety information must be surfaced without fear. Safety analysis will be conducted without blame.
7. Safety commitment, openness and honesty is valued and rewarded in the organization
8. Effective communication and the sharing of information is essential to preventing losses.

While these principles look deceptively simple, they actually take quite a bit of thought to create and are often not the principles actually guiding a company's decision making. More explanation behind them can be found in the STPA Handbook, Chapter 7.

시행 또는 서비스를 제공하는 사람들과는 독립적이며 상호작용이 적은 그룹에 의해 이루어지기도 한다. 문서 작업의 결과물은 파일로 저장되어 모든 사람들이 시스템이 안전하다는 것을 확신하게 한다.

- "허세(Swagger)" 문화: 안전은 약한 사람들(sissies)을 위한 것이다. 강한 사람들(real men)은 리스크를 통해 발전한다. 물론 여기서도 사고 방지와 관련된 문제는 명백하다.

어떤 조직이든 안전 문화는 최고 경영진에 의해 정해진다. 경영진의 안전에 대한 진정한 약속은 종종 안전을 달성하는 데 가장 중요한 요소로 언급된다. 직원들이 업무에서 안전에 대해 합리적인 우려를 표명하고 일정이나 비용과 같은 목표보다 안전을 우선시하면 지지를 받을 것이라고 느끼도록 해야 한다. 안전에 대한 우려는 때로는 입에 발린 말과 슬로건에 불과하다. 직원들은 빈말이 아니라 행동으로부터 그 신호를 받는다.

사고 조사 과정에서 안전 문화의 분석은 회사의 문서화 된 안전 철학 및 안전 정책 평가에서 시작되어야 한다. 이러한 것들이 존재하지 않는다면 분명히 문제가 있는 것이다. 필자는 의료 장비에서 심각한 안전 문제가 발견된 후 회사로부터 무슨 일이 있었는지 조사해 달라는 요청을 받았다. 이전에 그들에게 서면 안전 정책이 필요하다고 말했지만 그들은 그것을 만들지 않았다. 그들의 제품에 안전 문제가 발생한 후 나는 그 원인에 대해 물었고, 그들은 그들이 설계하고 판매하는 장비가 안전-중요 장비이므로 정책이 필요하지 않다는 것을 직원들에게 명확히 했어야 했다고 말했다. 동시에 제품의 다른 속성에 대한 서면 정책과 규칙은 많이 있었다. 또한 그들은 변호사들이, 안전 정책을 만들면 잠재적으로 제품이 위험하다는 것을 인정하는 것이기 때문에 안전 정책을 만들지 말 것을 조언했다고 하였다. 제품의 위험한 특성은 명백했으며, 누구도 안전 정책이 없다는 이유로 제품에 관련된 위험이 없다고 생각하지는 않았을 것이다. 그것은 단지 회사를 태만하게 보이게 했다. 내가 상담했던 사건 직후 회사는 파산하였고 없어졌다.

안전 철학은 경영진이 바라는 안전과 조직의 다른 목표들 간의 관계를 기술한 짧은 성명서이다. 안전 철학 성명서의 일반적인 원칙 중 일부 예는 다음과 같다:

1. 모든 부상과 사고는 방지할 수 있다.
2. 안전과 생산성은 밀접하게 관련되어 있다. 안전 관리를 개선하면 다른 품질 및 성능 요소가 향상된다. 비즈니스 성과를 극대화하려면 안전이 필요하다.
3. 안전은 제품 또는 서비스 설계에 내재되어야 한다. 이를 뒤늦게 추가하게 되면 효과가 떨어지고 비용이 많이 든다. 안전이 없는 설계에 대해 사후 보증을 통해 안전을 보장할 수는 없다. 사후에 안전을 확보하는 것보다 사전에 안전을 구축하는 것이 좋다.
4. 사건/사고 인과관계 분석의 목표는 책임질 누군가 또는 어떤 것을 찾는 것이 아닌, 손실(또는 니어 미스)이 발생한 이유를 파악하여 적절한 개선이 이루어지도록 하는 것이다.
5. 사건과 사고는 시스템이 안전하게 작동하지 않는 것을 알 수 있는 중요한 기회이며, 포괄적인 원인 분석 및 개선 조치의 시발점이 되도록 해야 한다.
6. 안전 정보는 두려움 없이 드러나야 한다. 안전 분석은 비난 없이 수행될 것이다.
7. 안전 약속, 솔직함 및 정직함은 조직 내에서 가치 있는 것이며 보상 받을 것이다.
8. 효과적인 의사소통과 정보 공유는 손실을 방지하는 데 필수적이다.

이런 원칙들은 매우 단순해 보이지만 실제로 만드는 데에는 많은 고민이 필요하며 회사의 의사결정을 가이드하는 원칙이 아닐 때도 있다. STPA 핸드북 7장에서 그에 대한 더 많은 설명을 하였다.

The safety philosophy establishes the principles upon which the more extensive safety policies and standards are built and assessed and provides a succinct statement of how management wants employees to make safety-related decisions and to act.

Of course, simply having a written philosophy does not mean that there has been buy-in by management and other employees. Do the managers actually implement the philosophy in their daily practices? Is there any process for ensuring that the philosophy is adopted and the principles practiced? How are the principles communicated to the employees? A written statement of the safety philosophy and more detailed policy statements and standards is a start, but it is not enough. Employees quickly identify when the written policy differs from the actual behavior of management. Do employees believe those at the top of the organization are sincerely committed to safety and are not just sloganeering and going through the motions? Asking some simple questions can identify when a deficient safety culture contributes to accidents.

While accident investigations sometimes use elaborate employee surveys to understand the existing safety culture, I have never found them useful. Writing down in a survey what one thinks they should say or believe does not mean that they actually think or act in that manner. I find that observing actual behavior is much more enlightening. Safety culture is best evaluated by studying management and employee behavior directly. How people behave is a much better indicator of their internal value system than what they answer on surveys.

How is commitment demonstrated? It is shown by setting priorities and following through on them; by personal involvement (e.g., top management chairing groups where safety decisions are made or at least getting personally involved); by setting up appropriate organizational structures; by appointing designated, high-ranking leaders to safety-related responsibilities and providing adequate resources for them to be effective; by assigning the best employees to safety-related activities and rewarding them for their efforts; and by responding to initiatives by others. It is also communicated by minimizing blame. Leaders need to demonstrate that their highest priority is to fix the systemic factors leading to losses and not just to find someone on which to pin blame (usually someone at the lowest levels in the organization) and then moving on when incidents or accidents occur. Finally, the incentive structure in the organization should be designed to encourage the behavior desired. Again, asking some questions about these factors during an accident investigation can provide insight into the contribution of the safety culture to the events. Does management value safety enough to use it as an important criterion when making decisions about promotions and raises?

## Changes and Dynamics over Time: In the System and in the Environment

Accidents usually occur after some type of change. The changes may be in the physical process, the operating procedures, individual behavior, the safety activities or processes, the management process, oversight practices (both internal and external), or in the environment in which the system exists and with which it must interact.

Changes may be planned or unplanned. Both types of changes need to be controlled and can lead to accidents if they are not.

If the changes are planned, a strong and well-designed management of change policy that is enforced and followed should be in place. In many accidents, management of change (MOC) procedures existed, but they were neither effective nor enforced. Examples in the Shell Moerdijk explosion include the switch to a new catalyst without testing it and assuming that previous catalyst properties still held and the removal of parts of the work instructions for Unit 4800 (again without assessment) because they were not considered critical. Critical requirements regarding nitrogen flow were removed during periodic updates of the work instructions in an attempt to limit their content to information that was

안전 철학은 보다 광범위한 안전 정책과 표준이 생성되고 평가되도록 그 원칙을 수립하고, 경영진이 원하는 직원의 안전-관련 결정 및 행동 방법에 대한 간결한 성명서를 제공한다.

물론 서면 철학을 가지고 있다는 것이 경영진과 다른 직원들로 하여금 이를 받아들였다는 것을 의미하지는 않는다. 경영진이 실제로 일상적인 업무에서 그 철학을 실천하는가? 철학이 채택되고 원칙이 실행되도록 하는 프로세스가 있는가? 원칙은 직원들에게 어떻게 전달되는가? 안전 철학에 대한 성명서와 상세한 정책 성명서 및 표준은 시작에 불과하며 그것만으로는 부족하다. 직원들은 서면 정책이 경영진의 실제 행동과 다를 때 이를 빠르게 파악한다. 직원들은 조직의 최상위에 있는 사람들이 안전에 진정으로 최선을 다하고 있으며 단지 슬로건만 가진 것이 아닌 행동으로 옮기고 있다고 생각하는가? 간단한 질문 몇 가지를 통해 안전 문화가 사고에 기여하는 시기를 알 수 있다.

사고 조사에서는 기존의 안전 문화를 이해하기 위해 정교한 직원 설문 조사를 활용하기도 하지만 그 결과가 유용했던 사례는 없었다. 자신이 말하거나 믿어야 한다고 생각하는 것을 설문지에 적는다고 해서, 실제로 그들이 그런 식으로 생각하거나 행동한다는 것을 의미하지는 않는다. 우리는 실제 행동을 관찰하는 것이 훨씬 더 많은 깨달음을 준다는 것을 알게 되었다. 안전 문화는 경영진과 직원의 행동을 직접 연구함으로써 가장 잘 평가할 수 있다. 설문 조사 답변보다 사람들의 행동 방식이 내부 가치 시스템을 훨씬 더 잘 확인할 수 있는 지표이다.

약속은 어떻게 증명되는가? 우선순위를 설정하고 그 순위대로 따름으로써 증명된다; 개인이 개입함으로써(예: 안전 결정이 내려지는 최고 경영진 의장 그룹 또는 최소한 개인이 개입); 적절한 조직 구조를 설정함으로써; 안전 관련 책임에 고위급 리더를 임명하고 이들이 효과적으로 이행하도록 충분한 자원 제공함으로써; 최고의 직원들을 안전 관련 활동에 배정하고 그들의 노력에 대해 보상함으로써; 다른 사람들의 발의(initiatives)에 응답함으로써 증명된다. 그것은 또한 비난을 최소화함으로써 전달된다. 리더는 사건이나 사고가 발생했을 때 단순히 책임을 지울 사람(일반적으로 조직에서 가장 낮은 수준에 있는 사람)을 찾는 것이 아니라 손실로 이어지는 시스템적 요소를 고치는 것이 가장 우선이라는 것을 증명하고 계속 진행해야 한다. 마지막으로 조직의 인센티브 구조는 조직이 바라는 행동을 장려하도록 설계되어야 한다. 다시 말해 사고 조사 과정에서 이러한 요소에 대한 몇 가지 질문을 통해 안전 문화의 사건 기여에 대한 통찰력을 얻을 수 있다. 경영진이 승진이나 승급을 결정할 때 안전을 중요한 기준으로 삼을 정도로 안전을 중시하고 있는가?

### 시간에 따른 변경 및 변동성: 시스템 및 환경 내에서

사고는 대개 어떤 변경 이후에 일어난다. 변경은, 물리적 프로세스, 운영 절차, 개별적인 동작, 안전 활동 또는 프로세스, 관리 프로세스, 감독 업무(내부 및 외부 모두) 또는 시스템이 존재하고 상호작용해야 하는 환경에 있을 수 있다.

변경은 계획된 것이거나 계획되지 않은 것일 수 있다. 이 두 가지 유형의 변경은 컨트롤되어야 하고 그렇지 않으면 사고로 이어질 수 있다.

변경이 계획되면 변경 정책이 강제되고 준수될 수 있도록 강력하고 잘 설계된 관리가 이루어져야 한다. 많은 사고에서 변경관리(MOC) 절차가 존재했지만 효과적이지도 강제적이지도 않았다. 쉘 뫼르딕 폭발 사례에서는, 테스트 없이 새로운 촉매제로 바꾸고 이전의 촉매 특성이 여전히 유지되고 있다고 가정하였으며 Unit 4800 작업 지침의 일부를 중요하지 않은 것으로 간주하여 삭제하였다. 질소 유량과 관련된 중요 요구사항은 작업 지침의 주기적인 업데이트 과정에서, 필수적이라고 여겨지는 정보로 그 내용을 제한하고 안전 및 운영 관점에서 가장 중요하다고 잘못 생각한 정보에 초점을 맞추기

believed essential and to focus on what was incorrectly thought to be the most important from a safety and operational view. Other information was omitted from the work instructions because, over time, understanding of the most appropriate procedures related to Unit 4800 changed.

Changes impacting risk may also be unplanned. There needs to be a way to detect unplanned changes that affect safety and to prevent them from occurring. Detection may be accomplished by using leading indicators and safety-focused audits. There may also be periodic planned re-evaluation of assumptions underlying the original safety-related design features and management procedures. At Shell Moerdijk, the leading indicators (such as number of leaks) were inadequate and too narrow, audits did not seem to be effective, and assumptions about the properties of ethylbenzene established in 1977 were never revisited.

Changes may occur slowly over time, as occurred at Shell Moerdijk with the work instructions for Unit 4800. As the work instructions were amended before each turnaround, important information was omitted—in some cases intentionally and in others unintentionally. Examples include the nitrogen flow requirements mentioned above and the required heating rate for the reactor. Changes do not appear to have been reviewed by experts, but if they were, then the review process was flawed.

Changes may be known and planned in one system component but appear as unplanned and unknown changes to another component of the system. The change in composition of the catalyst was known by the catalyst manufacturer but not by Shell Moerdijk. Clearly communication is an important factor here.

Leading indicators are commonly used in some industries to identify when the system is migrating toward a state of higher risk. At Shell Moerdijk, as well as most chemical plants, leading indicators used may be common throughout the whole industry, in this case number of leaks. Their selection seems to be predicated primarily on ease of collection and lack of having any alternatives for creating more effective ones.

I have created a new approach to identifying leading indicators that I called "assumption-based leading indicators."[21] Briefly the idea is that certain assumptions are made during system development that are used to design safety into a system. When, over time, those assumptions no longer hold, then the organization is likely to migrate to a state of higher risk. Leading indicators, then, can be identified by checking the original safety-related assumptions during operations to make sure that they are still true. Systems will always change and evolve over time, as will the environment in which the system operates. Because changes are necessary and inevitable, processes must be created to ensure that safety is not degrading. This new approach to leading indicators is being evaluated by Diogo Castilho, a Ph.D. candidate at MIT, on airline operations.[22]

Changes may evolve slowly over time and their impact may not be obvious. In a CAST analysis of crash of a cargo aircraft while landing at Birmingham Airport, one factor implicated in the inadequate operation of the safety control structure as a whole was an increase in night cargo operations at airports. Is there as much weight placed on cargo aircraft safety as passenger aircraft. Is more concern shown for daylight operations than for operations in the early darkness, which may be complicated by fatigue? We found that historical assumptions about airport operations may need to be revisited in the light of changes to airline operations and traffic.

Informal (and even formal) risk assessment may change as time passes without a loss. The actual risk has probably not decreased, but our perception of it does. That leads to a change in priorities and in the

[21] Nancy Leveson, (2015), A systems approach to risk management through leading safety indicators, *Reliability Engineering and System Safety*, 136: 17-34, April.

[22] Diogo Silva Castilho, *A Systems-Based Model and Processes for Integrated Safety Management Systems*, Ph.D. Dissertation, Aeronautics and Astronautics, MIT, expected September 2019.

위해 제거되었다. 시간이 지남에 따라 Unit 4800에 가장 적합한 절차에 대한 이해가 변경되었기 때문에 작업 지침에서 또 다른 정보가 누락되었다.

리스크에 영향을 미치는 변경사항이 계획되지 않은 것일 수도 있다. 안전에 영향을 미치는 이러한 계획되지 않은 변경을 탐지하고 방지하기 위한 방법이 필요한데 선행지표와 안전 중심의 감사를 활용하여 탐지할 수 있다. 또한 원래의 안전-관련 설계 특성과 관리 절차의 기초가 되는 가정에 대해 주기적으로 계획하여 재평가 할 수 있다. 쉘 뫼르딕에서는 선행지표(누출 횟수와 같은)가 부적절하고 너무 편협했으며 감사가 효과적이지 않아 보였고 1977년에 확립된 에틸벤젠의 특성에 대한 가정이 재검토되지 않았다.

시간이 지남에 따라 변경이 천천히 발생할 수도 있는데, 쉘 뫼르딕의 Unit 4800 작업 지침이 그러하다. 각 턴어라운드 전에 작업 지침이 개정되면서 중요한 정보가 누락되었다-어떤 경우는 의도적으로 누락되었고 어떤 경우는 의도하지 않게 누락되었다. 예시로 위에서 언급한 질소 유량에 대한 요구사항과 반응로에 필요한 가열 속도를 들 수 있다. 변경 사항이 전문가들에 의해 검토된 것으로 보이지 않았지만 만약 검토되었다면 검토 프로세스에 결함이 있었을 것이다.

한 시스템 컴포넌트에 대한 알려지고 계획된 변경사항이 그 시스템의 다른 컴포넌트에게는 계획되지 않고 알 수 없는 변경사항으로 보일 수 있다. 촉매제의 구성에 대한 변경사항은 촉매제 제조업체에게는 알려진 것이지만 쉘 뫼르딕에게는 알 수 없는 것이었다. 여기서 의사소통은 명백히 중요한 요소이다.

선행지표(leading indicators)는 시스템이 높은 리스크 상태로 이동하는 시점을 식별하기 위해 일부 산업에서 일반적으로 사용된다. 쉘 뫼르딕과 대부분의 화학 플랜트에서 사용되는 선행지표는 전 산업에 걸쳐 공통적으로 사용될 수 있는데, 쉘 뫼르딕 사례에서의 선행지표는 누출횟수이다. 쉘 뫼르딕의 지표 선택은 주로 수집의 용이성에 근거하고, 더 효과적인 지표에 대한 대안이 부족하다는 것에 근거한 것으로 보인다.

필자는 "가정 기반의 선행지표"[21]라고 불리는 선행지표를 식별하기 위한 새로운 접근법을 만들었다. 아이디어를 간단히 말하면, 시스템 개발 과정에서 시스템에 안전을 설계하는 데 사용되는 특정한 가정이 생긴다는 것이다. 시간이 지나면서 이러한 가정이 더 이상 유지되지 않으면 조직의 리스크가 더 높아질 수 있다. 이 때, 운영 단계에서의 원래의 안전-관련 가정이 여전히 사실(true)인지를 체크함으로써 선행지표를 식별할 수 있다. 시스템은 항상 시간이 지나면 변경되고 진화하며 시스템이 작동하는 환경 또한 변한다. 변경은 필연적이고 불가피하기 때문에 안전이 저하되지 않도록 하는 프로세스를 만들어야 한다. 선행지표에 대한 새로운 접근방식은 항공사 운영과 관련된 내용으로 MIT 대학의 박사과정인 디오고 카스틸루(Diogo Castilho)가 연구하고 있다.[22]

변경사항은 시간이 지나면서 천천히 진화할 수 있으며 그 영향이 분명하지 않을 수 있다. 버밍엄(Birmingham) 공항의 화물 수송기기 착륙 중에 추락한 것에 대한 CAST 분석에서, 전체 안전 컨트롤 스트럭처의 잘못된 동작과 관련된 한 가지 요소는 공항의 야간 화물 운항 증가였다. 여객기만큼 화물 수송기의 안전에도 비중을 두고 있는가? 피로로 인해 더 복잡해질 수 있는 초저녁의 운영보다 낮 시간의 운영에 더 많이 관심 가지는가? 우리는 공항 운영에 대한 기존의 오래된 가정들이 항공사 운영 및 수송 변화를 고려하여 재검토될 필요가 있음을 알게 되었다.

---

21 Nancy Leveson, (2015), A systems approach to risk management through leading safety indicators, Reliability Engineering and System Safety, 136: 17-34, April.

22 Diogo Silva Castilho, A Systems-Based Model and Processes for Integrated Safety Management Systems, Ph.D. Dissertation, Aeronautics and Astronautics, MIT, 2019. 9 예정

resolution of conflicting goals. Indeed, the Space Shuttle losses can be partly explained in this way, particularly the Columbia accident. Unfortunately, a strange dynamic can arise where success at preventing accidents can actually lead to behavior and decision making that paradoxically increases risk. A circular dynamic occurs where safety efforts are successfully employed, the feeling grows that accidents cannot occur, which leads to reduction in the safety efforts, an accident, and then increased controls for a while until the system drifts back to an unsafe state and complacency again increases and so on.

The complacency factor is so common that safety control structures need to include ways to deal with it. SUBSAFE, the U.S. nuclear submarine safety program puts major emphasis on fighting this tendency and has been particularly successful in accomplishing this goal. Identifying the migration to states of higher risk is an important part of any accident investigation. Understanding the reason for this migration during an accident causal analysis in which unrealistic risk perception is involved can help to identify ways to design the safety control structure to prevent it or detect it when it occurs.

One way to combat this erosion of safety is to provide ways to maintain accurate risk assessments in the process models of the system controllers. The better information controllers have, the more accurate will be their process models and therefore their decisions. Accident analysis should involve a careful investigation of the accuracy of risk perception in the mental models of those controlling safety.

## Internal and external economic and related factors

Systemic factors contributing to accidents often involve both internal and external economic conditions such as external market competition or declining profits. Market conditions may lead to management reducing the safety margins and ignoring established safety practices. Usually, there are precursors signaling the increasing risks associated with these changes, but too often these precursors are not recognized.

Another common factor is reduction in the physical separation between people and dangerous processes. Hazardous facilities are usually originally placed far from population centers, but the population shifts after the facility is created. People want to live near where they work and do not like long commutes. Land and housing may be cheaper near smelly, polluting plants. In third world countries, utilities, such as power and water, and transportation may be more readily available near heavy industrial plants, as was the case at Bhopal. The lure of providing jobs and economic development may encourage government officials to downplay risks and not rigorously enforce their safety control and emergency response requirements.

Over time, the land available for building may only be available near dangerous parts of the plant, as happened at the Texas City refinery where trailers were built to house employee offices next to the ISOM tower that exploded in 2005. With increasing population, local emergency facilities, such as firefighting and medical resources, may lag behind the increasing requirements due to constraints on resources and other competing priorities.

These factors may relate to the system environment not covered previously in the analysis of the individual controllers or even other general systemic factors, particularly changes and dynamics over time. How was individual controller behavior affected by these factors? Obvious factors are financial and competition concerns as well as new products and markets. Some non-obvious factors might be fatigue and duty cycles, distraction by contract negotiations, poor morale on the part of the work force due to a variety of factors, pressures to increase productivity beyond a reasonable level, etc.

Sometimes processes are automated and the standard safety controls implemented by humans are not implemented in the automated processes. There is often a naïve belief that software is always safe because it doesn't "fail" or that computers are more reliable than humans and therefore will improve

비정형적인(정형적일때 조차도) 리스크 평가의 결과는 손실이 발생하지 않은 경우에도 시간이 지남에 따라 변경될 수 있다. 실제 리스크는 감소되지 않았더라도 리스크에 대한 인식은 감소할 수 있다. 이는 우선순위 및 상충되는 목표에 대한 해결의 변경으로 이어진다. 실제로 우주왕복선의 손실은 부분적으로 이런 식으로 설명될 수 있는데, 특히 컬럼비아 사고에서 그렇다. 불행하게도, 사고를 성공적으로 예방하는 것이 실제로는 역설적으로 리스크를 증가시키는 동작과 결정으로 이어지는 잘못된 변동성을 야기할 수도 있다. 안전 노력이 성공적으로 채택되는 경우에는 순환적 변동성이 발생할 수 있는데, 즉, 사고가 일어나지 않는다는 느낌이 강해지면 이로 인해 안전 노력이 줄어들고, 그로 인해 사고가 발생한다. 사고 발생 후에는 시스템이 안전하지 않은 상태로 되돌아가 안일함이 다시 높아질 때까지 잠시 동안 컨트롤이 증가되는 것이 되풀이 되는 것이다.

안일함과 관련된 요소는 너무 일반적이어서 안전 컨트롤 스트럭처에 이를 처리하기 위한 방법을 포함해야 한다. 미국의 핵잠수함 안전 프로그램인 SUBSAFE는 이러한 경향에 대처하는 데에 중점을 두고 있으며 특히 이러한 목표 달성에 성공적이었다. 높은 리스트 상태로의 전환을 식별하는 것은 사고 조사의 중요한 부분이다. 비현실적인 위험 인식이 개입되는 사고 원인 분석 과정에서 이러한 전환이 발생하는 이유를 이해하면 그것을 예방하거나 발생 시 탐지할 수 있는 안전 컨트롤 스트럭처 설계 방법을 식별하는 데 도움이 될 수 있다.

이러한 안전 저하를 극복하는 한 가지 방법은 시스템 컨트롤러의 프로세스 모델에서 정확한 리스크 평가를 유지하도록 방법을 제공하는 것이다. 컨트롤러가 보다 나은 정보를 가질수록 프로세스 모델 및 그에 따른 결정이 더 정확해질 것이다. 사고 분석에는 안전을 컨트롤하는 사람들의 멘탈 모델에서 그들이 리스크를 얼마나 정확히 인식하는지에 대한 면밀한 조사가 포함되어야 한다.

### 내·외부 경제 및 관련 요인

사고에 기여하는 시스템적 요인은 외부 시장의 경쟁이나 이익의 감소와 같은 내·외부의 경제 조건을 모두 수반하는 경우가 많다. 경영진은 시장 상황으로 인해 안전 마진을 줄이고 확립된 안전 관행을 무시할 수도 있다. 일반적으로 이러한 변경과 관련된 리스크의 증가를 알리는 전조(precursors)가 있지만 너무 자주 이러한 전조가 인지되지 않는다.

또 다른 공통적인 요인은 사람과 위험한 프로세스 간의 물리적 분리가 잘 안 되는 것이다. 위험 시설은 원래 인구 중심에서 멀리 떨어져 있지만 시설이 만들어진 후에 인구가 이동하게 된다. 사람들은 일하는 곳 근처에서 살고 싶어 하고 긴 통근 거리를 좋아하지 않는다. 냄새가 나고 오염이 심한 플랜트 근처에서는 토지 및 주택의 가격이 더 저렴해질 것이다. 보팔(Bhopal)의 경우와 같이 제3세계 국가에서는 중공업 플랜트 근처에서 전력, 수도, 교통 등의 공공시설을 더 쉽게 이용할 수 있다. 일자리 제공과 경제 개발에 대한 유혹은 공무원들로 하여금 위험을 대단치 않게 생각하고 그들의 안전 컨트롤과 비상 대응 요구사항을 엄격하게 시행하지 않도록 만들 수 있다.

시간이 지나면서 건축이 가능한 토지는 플랜트의 위험한 지역 근처만 남게 될 것이다. 텍사스 시 정유소가 2005년 폭발한 ISOM타워 옆에 직원 주택 용도로 트레일러를 건설했던 것이 그 예이다. 인구가 증가함에 따라 소방 및 의료 시설과 같은 지역 비상 시설은 자원 및 기타 경쟁 우선순위 제약으로 인해 수요 증가를 따라 잡지 못할 수 있다.

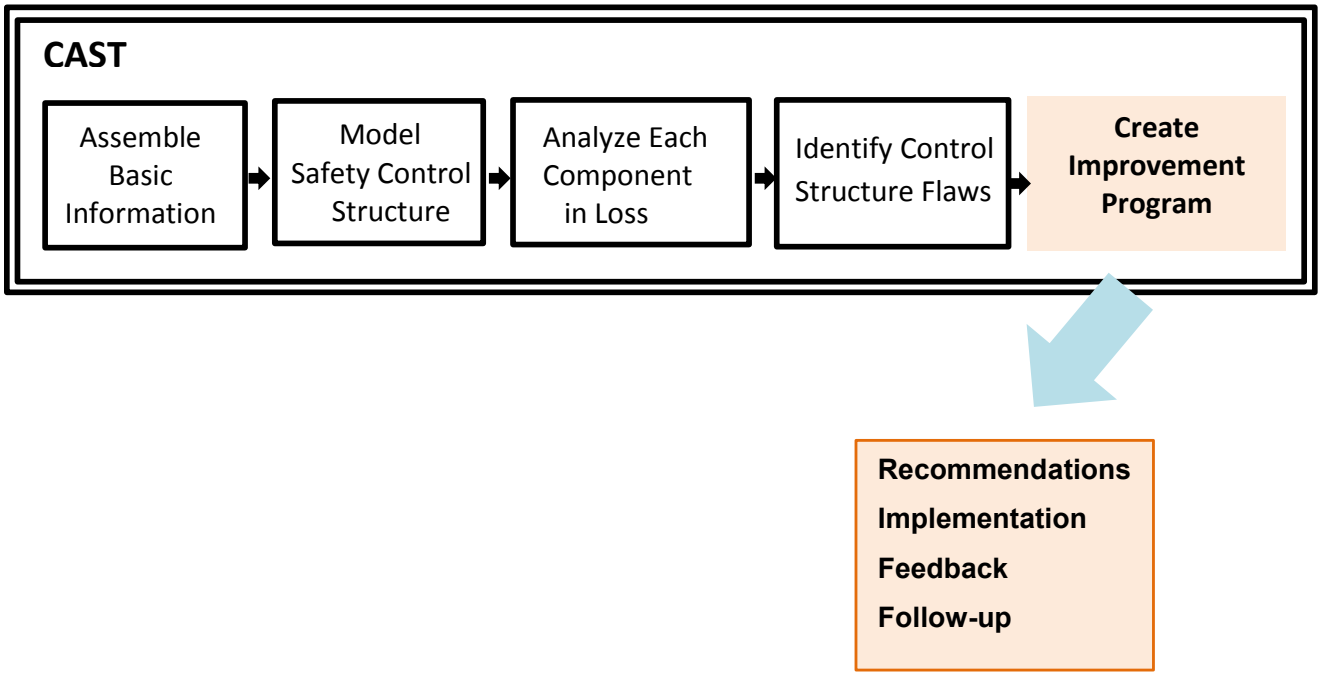
이러한 요인은 이전의 개별 컨트롤러의 분석에서 다루지 않았던 시스템 환경이나 다른 일반적인 시스템적 요인, 특히, 시간에 따른 변화와 변동성과 관련되어 있을 수 있다. 이러한 요인에 의해 개별 컨트롤러의 동작이 어떤 영향을 받았는가? 명백한 요인은 신제품이나 시장뿐만 아니라 재정 및 경쟁에

safety. Unfortunately, introducing automated systems introduces other changes into the system, often some that were not previously present. Complacency rises and new causes of accidents are introduced that are not controlled by the existing safety control structure.

대한 것이다. 일부 명백하지 않은 요인으로는 피로와 순환 근무, 계약 협상에 의한 혼동, 다양한 요인으로 인한 노동력의 사기저하, 합리적인 수준 이상으로 생산성을 높여야 한다는 압박 등이 포함된다.

때로는 프로세스가 자동화되어 사람이 구현한 표준 안전 컨트롤이 자동화된 프로세스에서는 실행되지 않는 경우가 있다. 소프트웨어는 “실패”하지 않으며 컴퓨터가 더 안정적이어서 안전이 향상될 것이므로, 소프트웨어가 항상 안전하다고 순진하게 믿는 경우가 종종 있다. 불행히도 자동화된 시스템을 도입하면 시스템에 다른 변경사항이 생기는데 그 중 일부는 이전에 존재하지 않았던 경우가 많다. 또한 안일함이 증가하고 기존 안전 컨트롤 스트럭처에 의해 컨트롤되지 않는 새로운 사고의 원인이 유입된다.

## Generating Recommendations and Changes to the Safety Control Structure



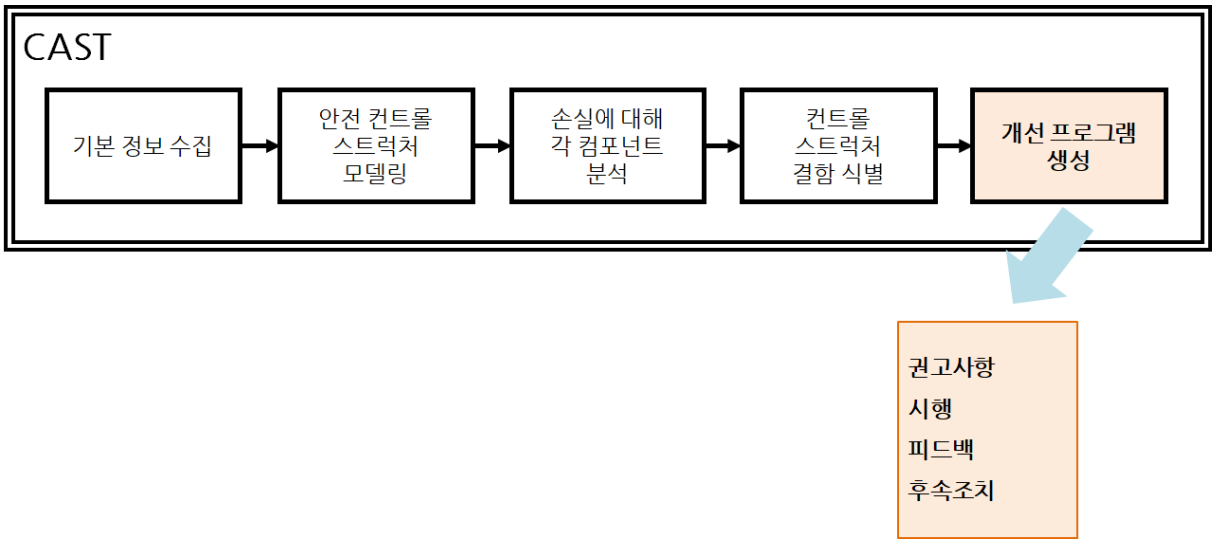

5. *Create recommendations for changes to the control structure to prevent a similar loss in the future. If appropriate, design a continuous improvement program for this hazard as part of your overall risk management program.*

*Generating Recommendations*

Once the other parts of the analysis are completed, generating recommendations should be straightforward. The biggest complaint about CAST we hear is that it generates too many recommendations. This complaint is only justified if the goal of the accident investigation is to make as few recommendations as possible. Accident investigation has had the goal of identifying "root causes" or "probable causes" for so long that it may be a cultural shock to start looking at more causal factors that generate more recommendations.

One of the objections raised to including a large number of recommendations is that responding to them is overwhelming. This is simply a logistical problem and not one that should be solved by learning less from each accident. There is no reason that recommendations cannot be prioritized according to specified criteria. There is also no implication that all the recommendations must be implemented immediately. Some recommendations will be relatively straightforward to implement immediately while others may take longer. Some may require such extensive changes that implementing them will take a great deal of effort and resources. Examples of the latter include establishing a new oversight agency or changing regulations and laws. Difficulty of implementation is not an excuse to omit a recommendation from the accident report, but it may be a good reason to categorize it as a longer-term goal rather than an immediate fix.

## 안전 컨트롤 스트럭처에 대한 권고사항 및 변경사항 작성




*5. 향후 유사한 손실을 방지하기 위해 컨트롤 스트럭처에 대한 변경 권고사항을 작성한다. 가능하면 전체적인 리스크 관리 프로그램의 일부로서 이 위험에 대한 지속적인 개선 프로그램을 설계한다.*

### *권고사항 생성(Generating Recommendations)*

분석이 완료되면 권고사항이 간단한 방법으로 도출될 수 있어야 한다. CAST에 대해 우리가 듣는 가장 큰 불만은 권고사항이 너무 많이 생성된다는 것이다. 하지만 이것은 사고 조사의 목표가 가능한 한 적은 권고사항을 만드는 경우에만 정당화될 수 있는 불만이다. 사고 조사는 너무 오랫동안 "근본 원인"이나 "가능한 원인"을 식별하는 것을 목표로 해 왔기 때문에 많은 권고사항을 생성하기 위한 더 많은 원인 요소를 찾는 것은 문화적 충격일 수 있다.

많은 수의 권고사항을 포함시키는 것에 대한 반대 의견 중 하나는 권고사항에 대한 대응이 지나치게 많이 요구된다는 것이다. 이것은 단순히 물량의 문제이며 각 사고로부터 적게 배우면서 해결해야 할 문제는 아니다. 특정한 기준에 따라 권고사항의 우선순위를 매길 수 없는 이유는 없다. 또한 모든 권고사항이 즉시 이행되어야 하는 것도 아니다. 일부 권고사항은 즉시 이행하는 것이 비교적 간단하지만 어떤 권고사항은 이행하는 데 오랜 시간이 걸릴 수도 있다. 권고사항 중 일부는 광범위한 변경을 필요로 할 수 있으므로 이를 이행하는 데 많은 노력과 자원이 필요할 수 있다. 후자의 예로는 새로운 감독 기관을 설립하거나 규정 및 법률을 변경하는 것이 있다. 이행의 어려움이 해당 권고사항을 사고 보고서에서 생략하기 위한 핑계가 될 수는 없으며, 즉각적인 수정 대신 장기적 목표로 분류하기 위한 좋은 근거가 될 수 있다.

단기적 해결책으로 "임시방편" 조치를 하는 것이 포괄적이고 효과적인 해결책을 계속적으로 지연시키는 이유가 되어서는 안 된다.

Taking steps to “jury-rig” short-term solutions should not be an excuse for endlessly delaying comprehensive and effective solutions.

*Establishing a Structure for Continual Improvement*

Sometimes recommendations are made but never implemented. Not only must there be some way to ensure recommendations are followed, there must also be feedback to ensure that they are effective in terms of achieving the goals and strengthening the safety control structure.

Essentially there are three requirements:

1. Assigning responsibility for implementing the recommendations
2. Checking that they have been implemented
3. Establishing a feedback system to determine whether they were effective in strengthening the controls.

The third requirement implies the need to collect evidence about the effectiveness of the recommended changes. Such feedback can come from audits and inspections and from the analysis of later incidents to determine whether previous recommendations were successful. Such an activity is a critical component of any safety management system, but it is often omitted.

Subsequent accidents or losses, particularly if they are analyzed using CAST, provide a rich source of information to understand why previous recommendations were not effective and what else is needed. Was the original causal analysis flawed? Were assumptions about the potential effectiveness of particular improvements incorrect? Did other changes occur that thwarted the attempt to strengthen the safety control structure? Did the planned changes result in unforeseen consequences?

The goal here is to ensure that your organization is continually learning and improving its risk management efforts so that the potential for losses is reduced over time.

### *지속적인 개선을 위한 구조 구축*

때로는 권고사항이 만들어져도 시행되지 않을 때가 있다. 권고사항을 준수할 수 있는 방법이 반드시 있어야 할 뿐만 아니라 목표를 달성하고 안전 컨트롤 스트럭처 강화 측면에서 효과가 있는지를 확인하기 위한 피드백이 있어야 한다.

기본적으로 다음과 같은 세 가지 요구사항이 있다.

1. 권고사항 시행에 대한 책임 할당
2. 권고사항이 시행되었는지 확인
3. 컨트롤 강화에 효과적인지 여부를 결정하기 위한 피드백 시스템 확립

세 번째 요구사항은 권고된 변경사항의 효과를 파악하기 위한 증거를 수집해야 함을 의미한다. 그러한 피드백은 감사와 검사 그리고 이전의 권고사항이 성공적이었는지를 파악하기 위한 이후의 사건 분석에서 나올 수 있다. 그러한 활동은 모든 안전 관리 시스템의 중요한 구성요소이지만 종종 생략되기도 한다.

후속 사고나 손실은, 특히 CAST를 사용하여 분석하였을 때, 이전의 권고사항이 효과적이지 못한 이유와 그 밖에 무엇이 필요했는지 파악할 수 있는 풍부한 정보 출처를 제공한다. 원래의 원인 분석에 결함이 있었는가? 특정 개선사항의 잠재적 효과에 대한 가정이 잘못되었는가? 안전 컨트롤 스트럭처를 강화하는 시도를 방해하는 다른 변경사항이 있었는가? 계획된 변경으로 인해 예상치 못한 결과가 발생하였는가?

여기서의 목표는 당신의 기업이 리스크 관리 노력을 지속적으로 배우고 개선하여 시간이 지남에 따라 손실 가능성을 감소시키는 것이다.

## Suggestions for Formatting the CAST Results

In STAMP, losses involve complex processes, not just a simple chain of events or even combination of event chains. The interactions among the events and causal factors are often intricate and subtle or indirect. In the end, it may be infeasible to list them as separate factors but only to understand the relationships among them. As a result, the format for presenting CAST results should emphasize the relationships among the various causal factors rather than a simple list, although lists are often difficult to avoid.

Tools for storing and organizing the results of a CAST analysis could easily be created, with extensive use of hyperlinks to show the relationships between various factors and behaviors and the location of answers to generated questions throughout the CAST analysis. More difficult, however, is coming up with a satisfactory standard notation for the presentation of the CAST results.

The goal is, of course, to provide the reader with an understanding of all the causal factors involved and how they all relate to each other. Different notations have had advantages in different accident analyses, with none that we have found working best for all of them.

As a result, documenting all the details of the analysis can use various types of notation, but readability and comprehensibility are important in a final summary of the causes of the accident. While all the details may not be necessary, there needs to be a way to present critical conclusions and argument. Trying to fit this all on a page (as with AcciMap analyses) leads to oversimplification and omission of important information. On the other hand, spreading the information over too many pages may lead to information overload and missing the bigger picture. I present here only a couple of examples that I have used and leave it for others to come up with better ideas.

For the Shell Moerdijk accident, I used the following format: a colored safety control structure with a table using colors as links to the summary analyses of the components as can be seen in Appendix B.

Alternatively, I have tried to insert the most important summary information in the control structure itself. Several figures from my analysis of a friendly fire accident where a U.S. F-15 shot down a U.S. Black Hawk helicopter over the Iraqi No-Fly-Zone are included here. The first shows the actions and analysis for the pilots, i.e., the F-15 lead pilot, the F-15 wing pilot, and the Black Hawk pilots. The second shows the analysis of the director of the ACE (the Airborne Command Element) up in the AWACS aircraft, who was commanding traffic in the area. The Mission Director was on the ground and overseeing the activities of the ACE. The third figure shows the analysis of the AWACS crew. Each of these figures is described in much more detail with accompanying text in the actual CAST analysis report. The notation does, however, allow an overview of the analysis. The additional text in the full CAST report should provide important but more detailed information.

## CAST 결과의 형식 제안

STAMP에서 손실은 단순히 이벤트 체인 또는 이벤트 체인의 조합뿐만 아니라 복잡한 프로세스와 관련되어 있다. 이벤트와 원인 요소들 간의 상호작용은 때론 복잡하고 미묘하거나 간접적이다. 결국, 그들 사이의 관계를 이해하기 위해 별개의 요소로 나열하는 것은 불가능할 것이다. 결론적으로 CAST 결과를 목록 형식으로 제시하는 것을 피하기 어려운 경우가 많지만 단순한 목록보다는 다양한 원인 요소 간의 관계가 강조되어야 한다.

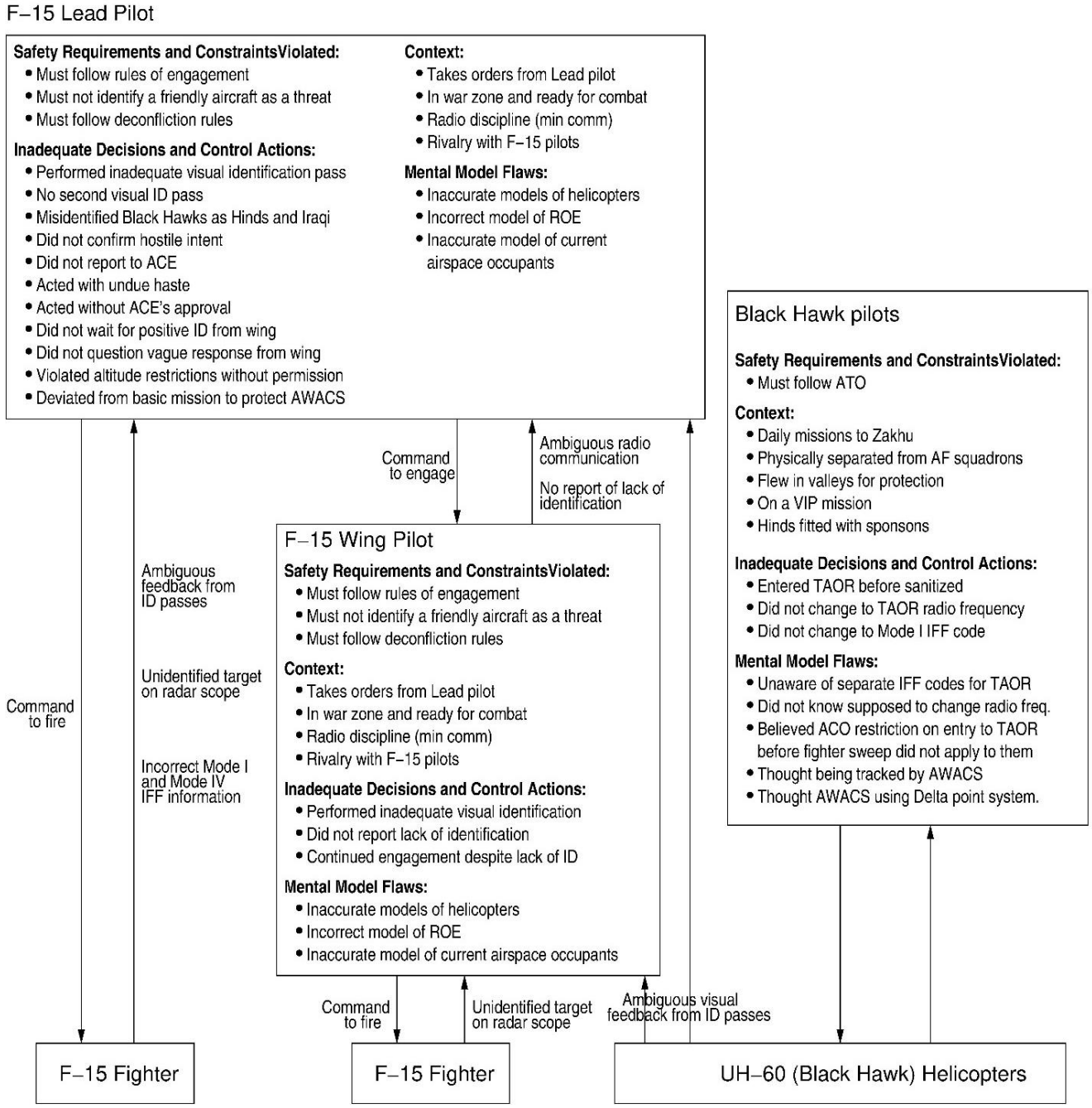
CAST 분석 결과를 저장하고 구조화하는 도구는 쉽게 만들 수 있다. 다양한 요인과 동작간의 관계, 그리고 CAST 분석 전체에서 생성된 질문에 대한 답변이 어디에 있는지를 보여주는 하이퍼링크를 폭넓게 사용하는 것이다. 그러나 더 어려운 것은, CAST 결과를 표시하기 위한 만족스러운 수준의 표준 표기법을 마련하는 것이다.

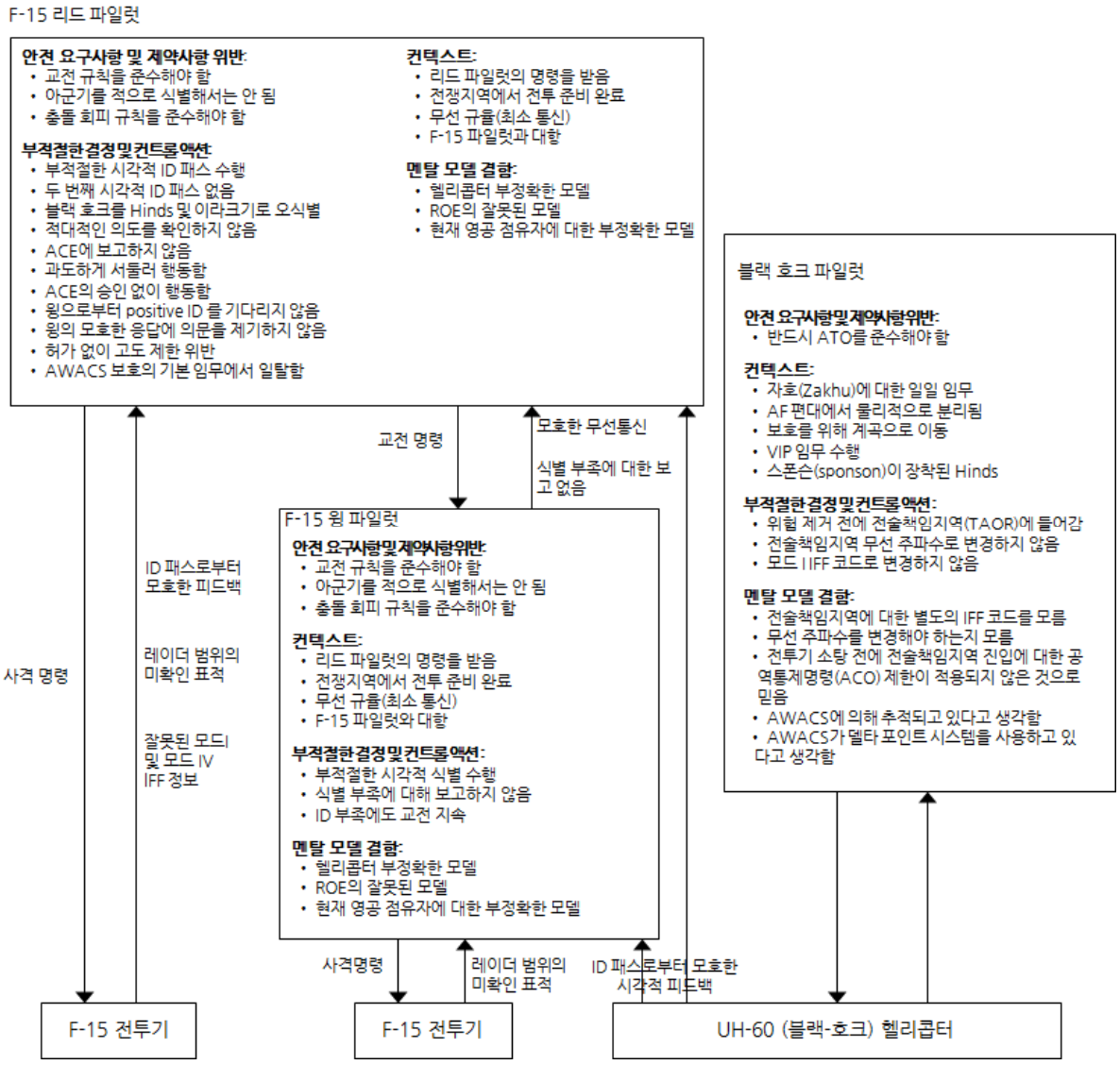
물론 목표는 독자들로 하여금 관련된 모든 원인 요소와 그것들이 어떻게 서로 연관되어 있는지를 이해하도록 하는 것이다. 각각의 여러 다른 표기법은 각기 다른 사고 분석에서 이점이 있었지만 가장 적합하다고 생각되는 것은 없었다.

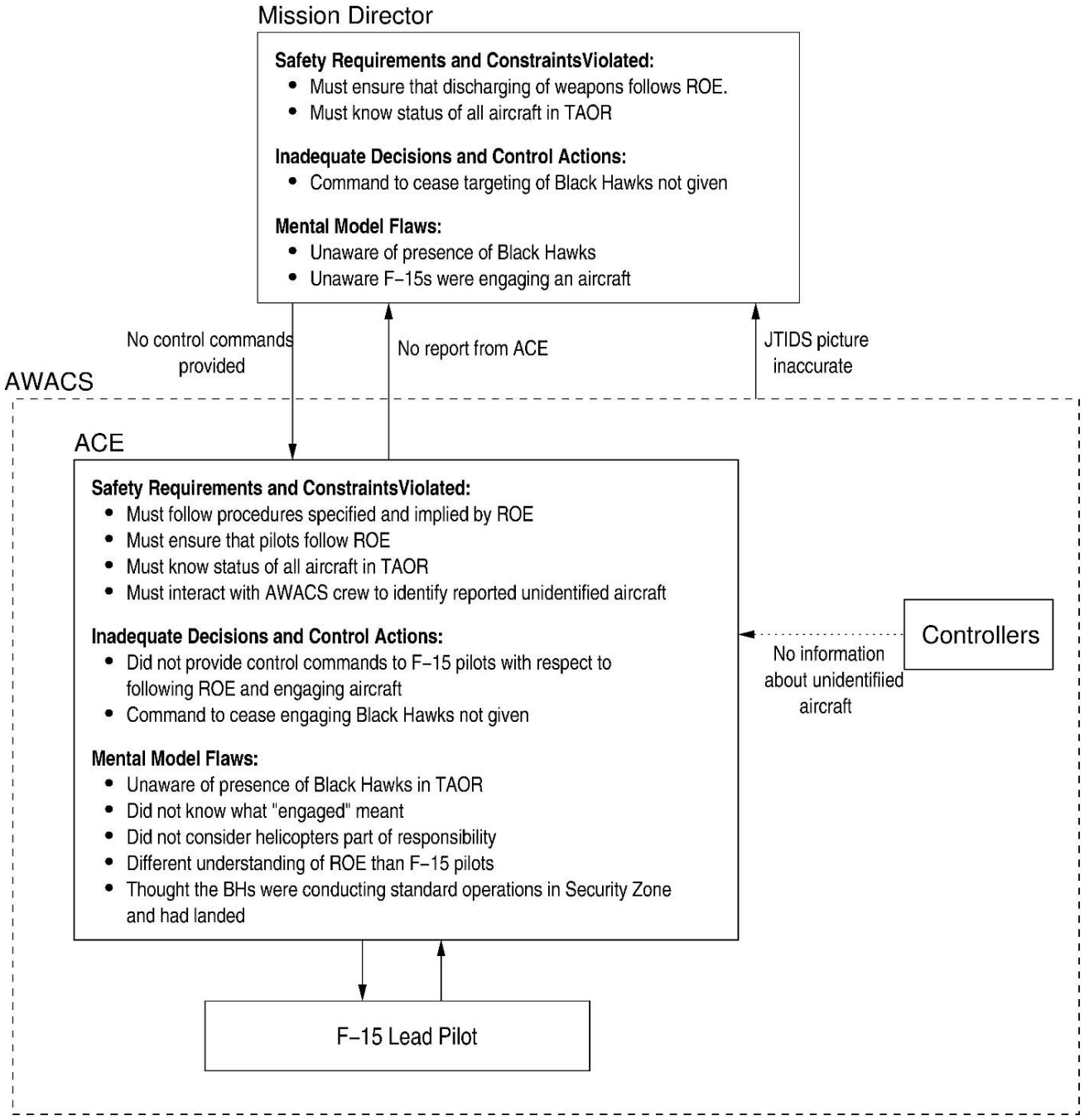
결과적으로 분석의 모든 세부사항을 문서화할 때 다양한 유형의 표기법을 사용할 수 있지만 사고 원인에 대한 최종 요약 부분에서는 가독성 및 이해도가 중요하다. 모든 세부사항들이 필요하지는 않지만 비판적인 결론과 주장을 제시할 방법은 필요하다. 한 페이지에 이 모든 것을 제시하려고 하면 (AcciMap 분석과 마찬가지로) 중요한 정보가 지나치게 단순화되거나 누락되는 경우가 발생한다. 반면에 너무 많은 페이지에 정보를 분산하여 제시하면 정보가 과부하되어 더 큰 그림을 놓치게 될 수도 있다. 여기에는 기존에 사용한 몇 가지 사례만을 제시하고 각자 더 나은 아이디어를 생각해 낼 수 있도록 남겨두도록 하겠다.

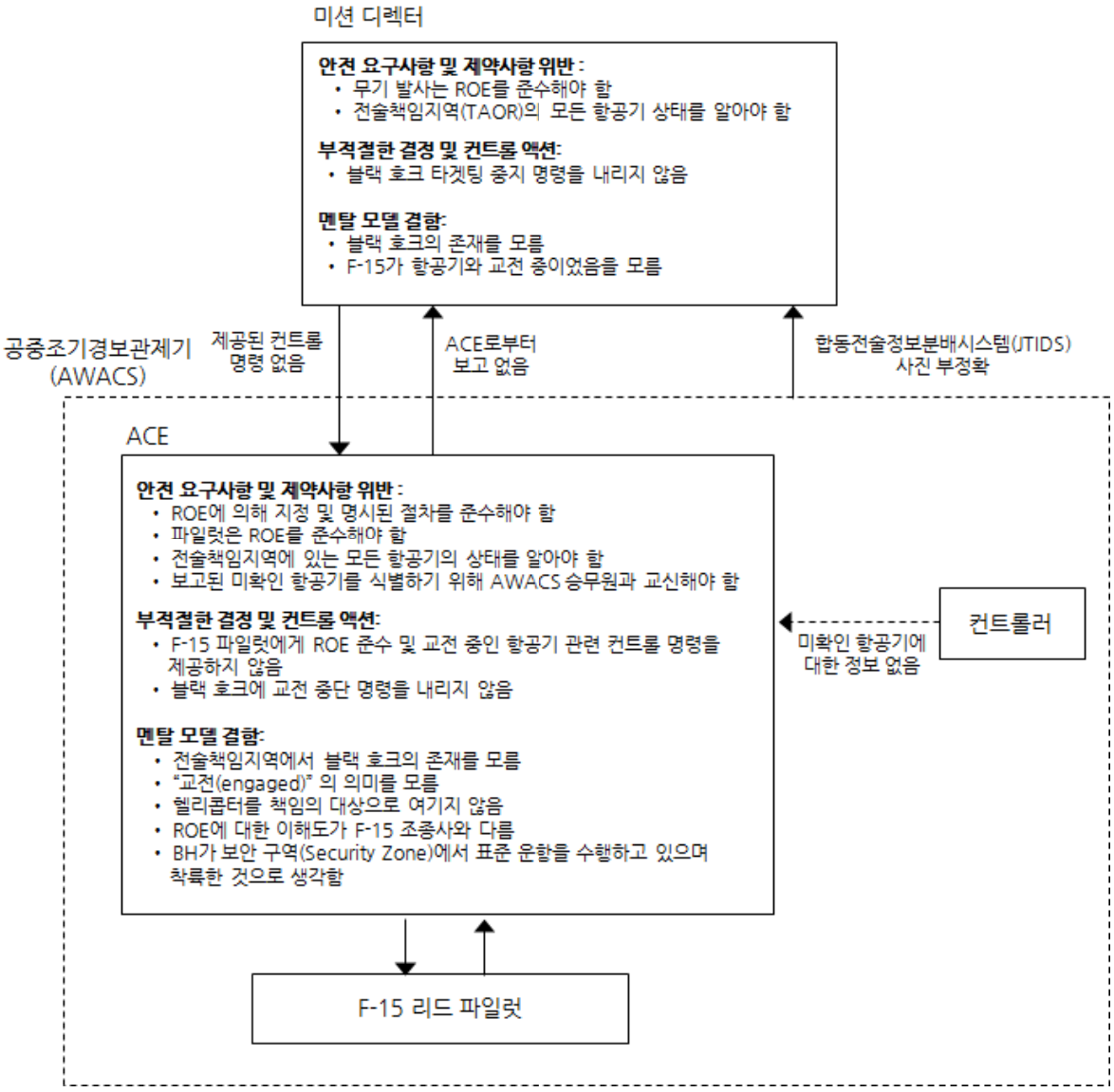
쉘 뫼르딕 사고의 경우 다음의 형식을 사용했다: 부록 B에서 볼 수 있듯이, 안전 컨트롤 스트럭처의 컴포넌트 색과, 컴포넌트에 대한 분석 요약 정보가 기재된 테이블의 색을 같은 색으로 표시함.

또한 컨트롤 스트럭처 자체에 가장 중요한 요약 정보를 삽입하려고 했다. 이라크 비행 금지 구역(No-Fly-Zone) 상공에서 U.S. F-15 전투기가 U.S. 블랙호크(Black Hawk) 헬기를 격추시킨 아군 포격 사고 분석에 대한 몇 가지 그림이 아래에 나와 있다. 첫 번째 그림은 파일럿, 즉, F-15 리드 파일럿, F-15 윙 파일럿, 블랙호크 파일럿의 행동 및 그 분석을 보여준다. 두 번째 그림은 해당 지역의 운항을 통제하고 있는 AWACS 항공기의 ACE(Airbone Command Element) 책임자에 대한 분석을 보여준다. 미션 디렉터(Mission Director)는 지상에서 ACE의 활동을 감독하고 있었다. 세 번째 그림은 AWACS 승무원에 대한 분석을 보여준다. 각각의 그림들은 실제 CAST 분석 보고서에서 텍스트와 함께 훨씬 자세히 설명된다. 이러한 표기법으로 분석에 대한 개요를 보여줄 수 있기는 하나, 전체 CAST 보고서에서 추가적인 텍스트를 이용하여, 중요하며 보다 상세한 정보를 제공해야 한다.


F–15 Lead Pilot
Safety Requirements and ConstraintsViolated:
• Must follow rules of engagement
• Must not identify a friendly aircraft as a threat
• Must follow deconfliction rules
Inadequate Decisions and Control Actions:
• Performed inadequate visual identification pass
• No second visual ID pass
• Misidentified Black Hawks as Hinds and Iraqi
• Did not confirm hostile intent
• Did not report to ACE
• Acted with undue haste
• Acted without ACE's approval
• Did not wait for positive ID from wing
• Did not question vague response from wing
• Violated altitude restrictions without permission
• Deviated from basic mission to protect AWACS
Context:
• Takes orders from Lead pilot
• In war zone and ready for combat
• Radio discipline (min comm)
• Rivalry with F–15 pilots
Mental Model Flaws:
• Inaccurate models of helicopters
• Incorrect model of ROE
• Inaccurate model of current airspace occupants
Black Hawk pilots
Safety Requirements and ConstraintsViolated:
• Must follow ATO
Context:
• Daily missions to Zakhu
• Physically separated from AF squadrons
• Flew in valleys for protection
• On a VIP mission
• Hinds fitted with sponsons
Inadequate Decisions and Control Actions:
• Entered TAOR before sanitized
• Did not change to TAOR radio frequency
• Did not change to Mode I IFF code
Mental Model Flaws:
• Unaware of separate IFF codes for TAOR
• Did not know supposed to change radio freq.
• Believed ACO restriction on entry to TAOR before fighter sweep did not apply to them
• Thought being tracked by AWACS
• Thought AWACS using Delta point system.
Command to engage
Ambiguous radio communication
No report of lack of identification
F–15 Wing Pilot
Safety Requirements and ConstraintsViolated:
• Must follow rules of engagement
• Must not identify a friendly aircraft as a threat
• Must follow deconfliction rules
Context:
• Takes orders from Lead pilot
• In war zone and ready for combat
• Radio discipline (min comm)
• Rivalry with F–15 pilots
Inadequate Decisions and Control Actions:
• Performed inadequate visual identification
• Did not report lack of identification
• Continued engagement despite lack of ID
Mental Model Flaws:
• Inaccurate models of helicopters
• Incorrect model of ROE
• Inaccurate model of current airspace occupants
Ambiguous feedback from ID passes
Unidentified target on radar scope
Incorrect Mode I and Mode IV IFF information
Command to fire
Command to fire
Unidentified target on radar scope
Ambiguous visual feedback from ID passes
F–15 Fighter
F–15 Fighter
UH–60 (Black Hawk) Helicopters


F-15 리드 파일럿
안전 요구사항 및 제약사항 위반:
• 교전 규칙을 준수해야 함
• 아군기를 적으로 식별해서는 안 됨
• 충돌 회피 규칙을 준수해야 함
부적절한 결정 및 컨트롤 액션:
• 부적절한 시각적 ID 패스 수행
• 두 번째 시각적 ID 패스 없음
• 블랙 호크를 Hinds 및 이라크기로 오식별
• 적대적인 의도를 확인하지 않음
• ACE에 보고하지 않음
• 과도하게 서둘러 행동함
• ACE의 승인 없이 행동함
• 윙으로부터 positive ID 를 기다리지 않음
• 윙의 모호한 응답에 의문을 제기하지 않음
• 허가 없이 고도 제한 위반
• AWACS 보호의 기본 임무에서 일탈함
컨텍스트:
• 리드 파일럿의 명령을 받음
• 전쟁지역에서 전투 준비 완료
• 무선 규율(최소 통신)
• F-15 파일럿과 대항
멘탈 모델 결함:
• 헬리콥터 부정확한 모델
• ROE의 잘못된 모델
• 현재 영공 점유자에 대한 부정확한 모델
블랙 호크 파일럿
안전 요구사항 및 제약사항 위반:
• 반드시 ATO를 준수해야 함
컨텍스트:
• 자호(Zakhu)에 대한 일일 임무
• AF 편대에서 물리적으로 분리됨
• 보호를 위해 계곡으로 이동
• VIP 임무 수행
• 스폰슨(sponson)이 장착된 Hinds
부적절한 결정 및 컨트롤 액션:
• 위협 제거 전에 전술책임지역(TAOR)에 들어감
• 전술책임지역 무선 주파수로 변경하지 않음
• 모드 I IFF 코드로 변경하지 않음
멘탈 모델 결함:
• 전술책임지역에 대한 별도의 IFF 코드를 모름
• 무선 주파수를 변경해야 하는지 모름
• 전투기 소탕 전에 전술책임지역 진입에 대한 공역통제명령(ACO) 제한이 적용되지 않은 것으로 믿음
• AWACS에 의해 추적되고 있다고 생각함
• AWACS가 델타 포인트 시스템을 사용하고 있다고 생각함
교전 명령
모호한 무선통신
식별 부족에 대한 보고 없음
F-15 윙 파일럿
안전 요구사항 및 제약사항 위반:
• 교전 규칙을 준수해야 함
• 아군기를 적으로 식별해서는 안 됨
• 충돌 회피 규칙을 준수해야 함
컨텍스트:
• 리드 파일럿의 명령을 받음
• 전쟁지역에서 전투 준비 완료
• 무선 규율(최소 통신)
• F-15 파일럿와 대항
부적절한 결정 및 컨트롤 액션:
• 부적절한 시각적 식별 수행
• 식별 부족에 대해 보고하지 않음
• ID 부족에도 교전 지속
멘탈 모델 결함:
• 헬리콥터 부정확한 모델
• ROE의 잘못된 모델
• 현재 영공 점유자에 대한 부정확한 모델
ID 패스로부터 모호한 피드백
레이더 범위의 미확인 표적
잘못된 모드I 및 모드 IV IFF 정보
사격 명령
사격명령
레이더 범위의 미확인 표적
ID 패스로부터 모호한 시각적 피드백
F-15 전투기
F-15 전투기
UH-60 (블랙-호크) 헬리콥터


Mission Director
Safety Requirements and ConstraintsViolated:
Must ensure that discharging of weapons follows ROE.
Must know status of all aircraft in TAOR
Inadequate Decisions and Control Actions:
Command to cease targeting of Black Hawks not given
Mental Model Flaws:
Unaware of presence of Black Hawks
Unaware F–15s were engaging an aircraft
No control commands provided
No report from ACE
JTIDS picture inaccurate
AWACS
ACE
Safety Requirements and ConstraintsViolated:
Must follow procedures specified and implied by ROE
Must ensure that pilots follow ROE
Must know status of all aircraft in TAOR
Must interact with AWACS crew to identify reported unidentified aircraft
Inadequate Decisions and Control Actions:
Did not provide control commands to F–15 pilots with respect to following ROE and engaging aircraft
Command to cease engaging Black Hawks not given
Mental Model Flaws:
Unaware of presence of Black Hawks in TAOR
Did not know what "engaged" meant
Did not consider helicopters part of responsibility
Different understanding of ROE than F–15 pilots
Thought the BHs were conducting standard operations in Security Zone and had landed
Controllers
No information about unidentifiied aircraft
F–15 Lead Pilot


미션 디렉터
안전 요구사항 및 제약사항 위반 :
• 무기 발사는 ROE를 준수해야 함
• 전술책임지역(TAOR)의 모든 항공기 상태를 알아야 함
부적절한 결정 및 컨트롤 액션:
• 블랙 호크 타겟팅 중지 명령을 내리지 않음
멘탈 모델 결함:
• 블랙 호크의 존재를 모름
• F-15가 항공기와 교전 중이었음을 모름
공중조기경보관제기 (AWACS)
제공된 컨트롤 명령 없음
ACE로부터 보고 없음
합동전술정보분배시스템(JTIDS) 사진 부정확
ACE
안전 요구사항 및 제약사항 위반 :
• ROE에 의해 지정 및 명시된 절차를 준수해야 함
• 파일럿은 ROE를 준수해야 함
• 전술책임지역에 있는 모든 항공기의 상태를 알아야 함
• 보고된 미확인 항공기를 식별하기 위해 AWACS 승무원과 교신해야 함
부적절한 결정 및 컨트롤 액션:
• F-15 파일럿에게 ROE 준수 및 교전 중인 항공기 관련 컨트롤 명령을 제공하지 않음
• 블랙 호크에 교전 중단 명령을 내리지 않음
멘탈 모델 결함:
• 전술책임지역에서 블랙 호크의 존재를 모름
• "교전(engaged)" 의 의미를 모름
• 헬리콥터를 책임의 대상으로 여기지 않음
• ROE에 대한 이해도가 F-15 조종사와 다름
• BH가 보안 구역(Security Zone)에서 표준 운항을 수행하고 있으며 착륙한 것으로 생각함
컨트롤러
미확인 항공기에 대한 정보 없음
F-15 리드 파일럿

AWACS Mission Crew

**Safety Requirements and ConstraintsViolated:**

- Must identify and track all aircraft in TAOR
- Friendly aircraft must not be misidentified as hostile
- Must accurately inform fighters about status of all aircraft when queried.
- Must alert fighters of any aircraft not appearing on flowsheet.
- Must not fail to warn fighters about any friendly aircraft they are targeting
- Must provide ground with accurate picture of airspace and its occupants (through JTIDS).

**Dysfunctional Interactions:**

- Control of aircraft not handed off from enroute to TAOR controller
- Interactions between ASO and senior WD with respect to tracking the flight of the helicopters on the radarscope.

**Inadequate Decisions and Control Actions:**

- Enroute controller did not tell BH pilots to change to TAOR frequency.
- Enroute controller did not hand off control of BHs to TAOR controller
- Enroute controller did not monitor course of BHs while in TAOR.
- Enroute controller did not use Delta point system to determine BH flight plan
- TAOR controller did not monitor course of helicopters in TAOR
- Nobody alerted F–15 pilots before they fired that the helicopters they were targeting were friendly.
- Nobody warned pilots that friendly aircraft were in the area.
- Did not try to stop the engagement
- Nobody told BH pilots that squawking wrong IFF code.
- MCC did not relay information that was not on ATO about helicopters during morning briefing.
- Shadow crew was not monitoring activities.

**Coordination Flaws:**

- Confusion over who was tracking helicopters
- Confusion over responsibilities of surveillance and weapon directors
- No one assigned responsibility for monitoring helicopter traffic in NFZ
- Confusion over who had authority to initiate engagement

**Context:**

- Min Comm
- Poor morale. inadequate training, over worked
- Low activity at time of accident
- Terminal failure led to changed seating arrangement
- Airspace violations were rare

**Mental Model Flaws:**

- Did not think helicopters were an integral part of OPC air operations.
- Inaccurate models of airspace occupants and where they were.
- Thought helicopters only going to Zakhu




Systemic factors can often be described effectively with figures. The communication losses in the Überlingen accident was shown using two figures (Figure 16 and 17): one showed the designed communication links and the other showed the links actually operable at the time of the accident. Missing and flawed feedback was shown in Figure 18 for the ComAir Lexington crash. Figures can also be an effective way to show important changes over time in the control structure. Figure 20 shows the original designed control structure involved in an E. coli contamination of a water supply in Walkerton Canada. The details are not important here. Figure 21 shows the control structure as it existed at the time of the accident. The greyed-out structures in Figure 21 show the parts of the control structure that were eliminated over time with the blue structures depicting additions.

공중조기경보관제기(AWACS) 승무원

**안전 요구사항 및 제약사항 위반:**
- 전술책임지역의 모든 항공기를 식별하고 추적해야 함
- 아군기가 적으로 잘못 식별되면 안 됨
- 전투기로부터 요청이 있는 경우 모든 항공기의 상태를 정확하게 알려야 함
- 플로우 시트에 나타나지 않은 항공기를 전투기에게 경고해야 함
- 전투기가 아군기를 타겟팅하고 있는 경우 반드시 경고해야 함
- 영공 및 영공 점유자의 정확한 사진을 지상에 제공해야 함(JTIDS를 통해)

**기능장애 상호작용:**
- 항공기 컨트롤이 항공로에서 전술책임지역 컨트롤러로 이관되지 않음
- 레이더스코프에서 헬리콥터의 비행 추적과 관련된 ASO와 수석 WD간의 상호작용

**부적절한 결정 및 컨트롤 액션:**
- 항공로 컨트롤러가 BH 조종사에게 전술책임지역 주파수로 변경하라고 말하지 않음
- 항공로 컨트롤러에서 전술책임지역 컨트롤러로 BH제어 권한을 양도하지 않음
- 전술책임지역에 있는 동안 항공로 컨트롤러가 BH의 경로를 모니터링 하지 않음
- 항공로 컨트롤러가 BH 비행계획을 결정하는 데 델타 포인트 시스템을 사용하지 않음
- 전술책임지역 컨트롤러가 전술책임지역의 헬리콥터 경로를 모니터링 하지 않음
- F-15 파일럿이 사격하기 전에 타겟팅하고 있는 헬리콥터가 아군이라는 것을 아무도 경고하지 않음
- 아군기가 그 지역에 있다는 것을 아무도 파일럿에게 경고하지 않음
- 교전을 중단하지 않음
- 아무도 BH 파일럿에게 잘못된 IFF 코드에 대해 알리지 않음
- 오전 브리핑에서 MCC가 ATO에 없는 헬리콥터 정보를 전달하지 않음
- 쉐도우 승무원이 활동을 모니터링하지 않음

**조정 결함:**
- 헬리콥터를 추적을 누가 하고 있는지에 대한 혼동
- 감시 및 무기 통제사(WD)의 책임에 대한 혼동
- NFZ 내 헬리콥터 운항에 대한 모니터링 책임자가 없음
- 교전 시작할 권한을 누가 가졌는지에 대한 혼동

**컨텍스트:**
- 최소한의 통신
- 사기 저하, 불충분한 훈련, 과로
- 사고 당시의 활동 저조
- 터미널 장애로 좌석 배치가 변경됨
- 공역 위반은 드물었음

**멘탈 모델 결함:**
- 헬리콥터가 OPC 항공 운영에 필수적인 부분이라고 생각하지 않음
- 영공 점유자 및 그 점유자가 있었던 곳에 대한 부정확한 모델
- 자호(Zakhu)로 향하는 헬리콥터만 고려함




시스템적 요소는 종종 그림을 사용하여 효과적으로 설명할 수 있다. 위버링겐 사고의 의사소통 손실은 두 개의 그림(그림 16과 17)을 사용하여 명시되었다: 하나는 설계된 의사소통 링크를 보여주었고 다른 하나는 사고 당시 실제로 작동할 수 있는 의사소통 링크를 보여주었다. 그림 18은 렉싱턴 공항에서의 ComAir 항공기 충돌에 대한 누락되었거나 결함 있는 피드백을 보여준다. 그림은 시간 경과에 따른 컨트롤 스트럭처의 중요한 변경사항을 보여주는 효과적인 방법이 될 수도 있다. 그림 20은 캐나다 워커톤(Walkerton)에서 물 공급원의 대장균(E. coli) 오염과 관련하여 원래 설계된 컨트롤 스트럭처를 보여준다. 여기서 세부사항은 중요하지 않다. 그림 21은 사고 당시의 컨트롤 스트럭처를 보여주고 있다. 그림 21의 회색으로 표시된 스트럭처는 시간 경과에 따라 없어진 컨트롤 스트럭처의 부분을 보여주며 추가된 컨트롤 스트럭처는 파란색으로 표시하고 있다.

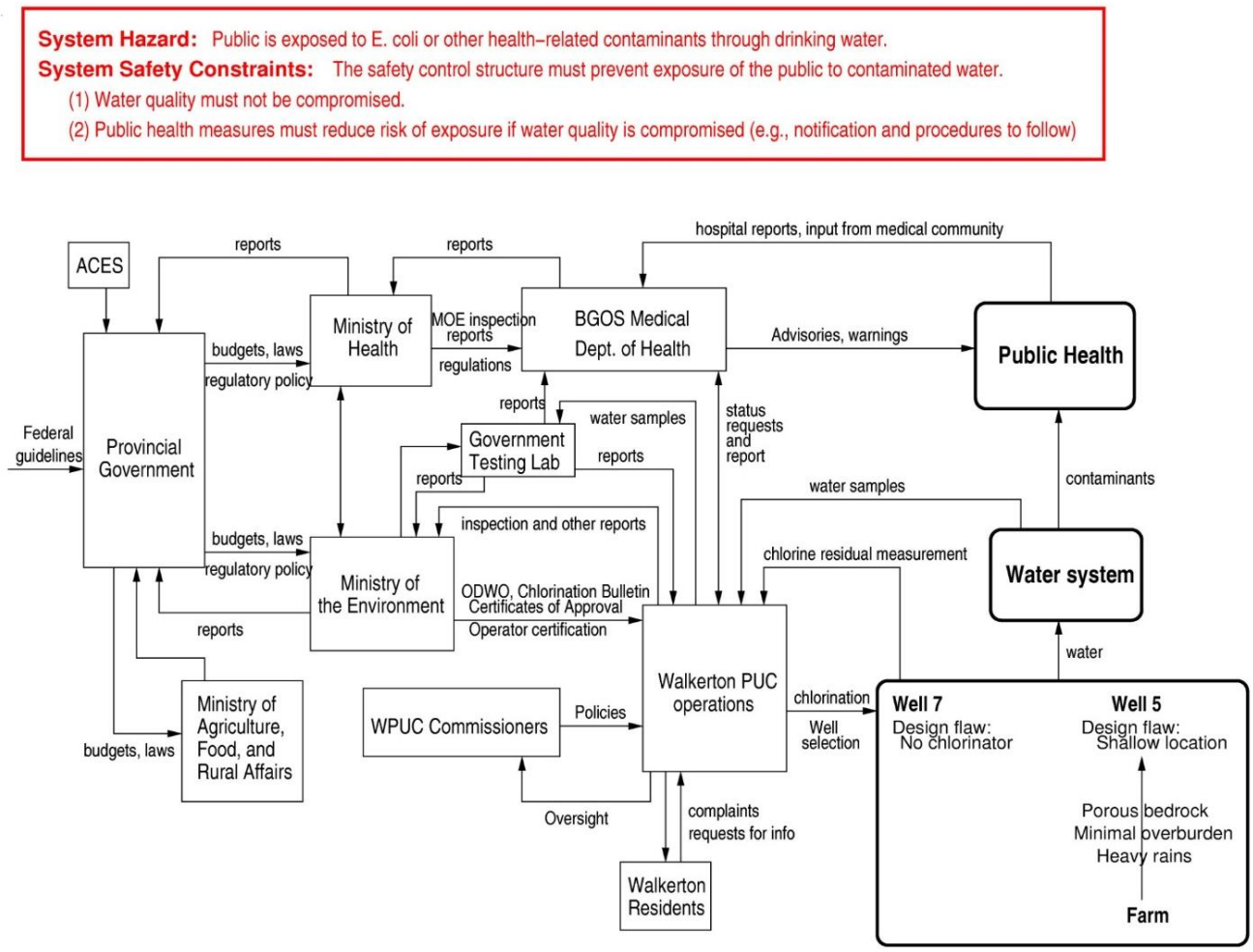



**Figure 20:** The original, designed control structure to control water quality in Ontario, Canada.

In this water contamination accident, a conservative government had been elected and decided to privatize the government water testing lab. This change would have been OK if the private labs had been required to inform the government about the results of their water testing. However, there was also an effort to reduce what was considered to be red tape and excessive reporting by private companies, so the private testing labs only reported their results directly to the operators overseeing water supply operations in Walkerton, who did not understand that water could be contaminated with E. coli. Figure 21 shows the resulting loss of all feedback about the behavior of the Walkerton operations by the Ministry of the Environment. By shading out the parts of the control structure that had disappeared, the problem is clearly depicted. While the Medical Dept. of Health might have been able to detect the problems, they assumed that the Ministry of the Environment was providing oversight and did not intervene. The blue parts of the control structure show the additions over time. Like any accident, the explanation is quite complicated. For one thing, although operator certification was instituted (which would have required additional education for the Walkerton operators), they were grandfathered out of new education and certification requirements.

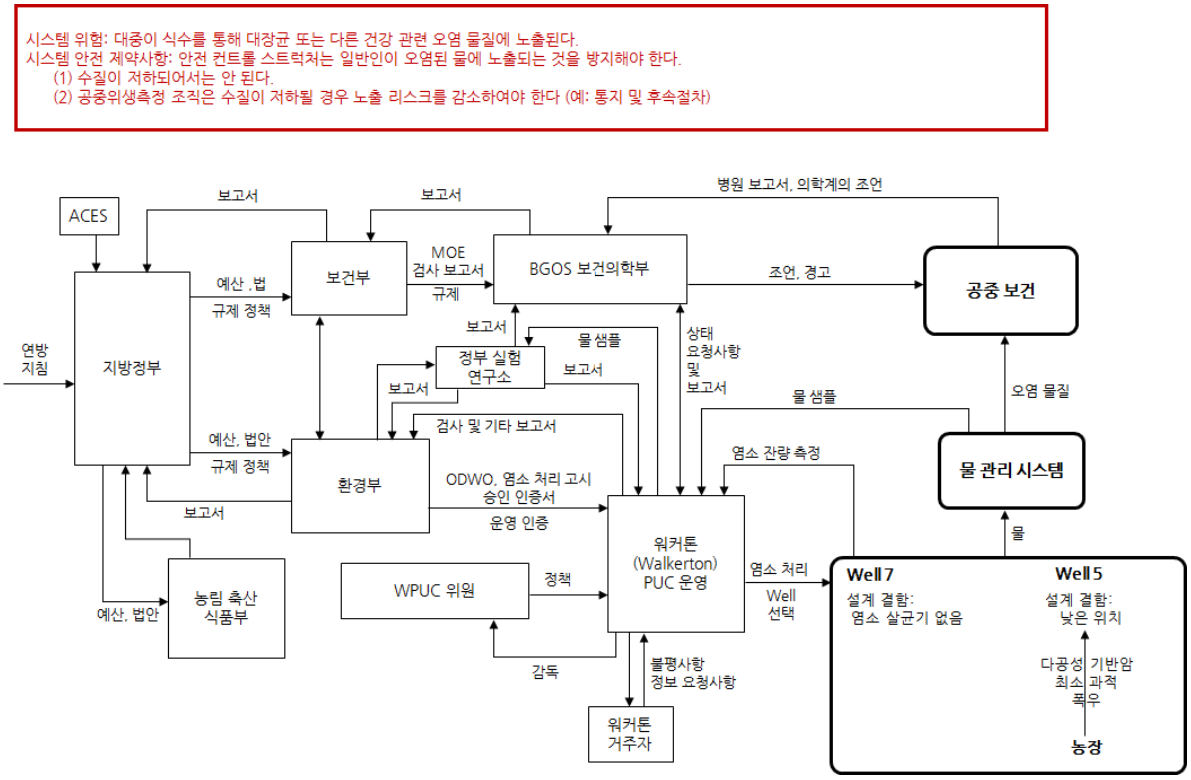



그림 20 : 캐나다 온타리오주의 수질 컨트롤을 위해 설계된 컨트롤 스트럭처 원본

이 수질 오염 사고는 선출된 보수 정부가 정부 수질 검사 연구소를 민영화하기로 결정한 부분과도 관련이 있다. 만약 사설 연구소가 정부에게 수질 검사 결과를 알려야 했다면 이러한 결정은 문제가 없었을 것이다. 그러나 사설 연구소에서는 불필요한 요식(red tape)이나 지나친 보고를 줄이려고 노력하였다. 이 때문에 사설 테스팅 연구소는 워커톤의 급수 운영 감독을 맡고 있는 운영자에게만 직접적으로 결과를 보고하였으며, 그 담당자는 물이 대장균에 오염될 수 있다는 것을 이해하지 못했다. 그림 21은 환경부에 대한 워커톤 운영의 모든 피드백이 손실된 결과를 보여준다. 사라졌던 컨트롤 스트럭처 부분을 음영 처리함으로써 문제를 명확하게 보여주고 있다. 보건부의 의료 부서가 이 같은 문제점을 탐지할 수 있었을지도 모르지만 환경부는 워커톤을 감시하고 있는 것으로 가정하여 개입하지 않았다. 컨트롤 스트럭처의 파란색 부분은 시간이 지남에 따른 추가사항을 보여준다. 여느 사고와 마찬가지로 설명은 상당히 복잡하다. 한 가지 예로, 운영자 인증(워커톤 운영자를 위한 추가 교육이 요구되는 인증)이 마련되었지만 그 인증은 새로운 교육 및 인증 요구사항에서 제외되었다.

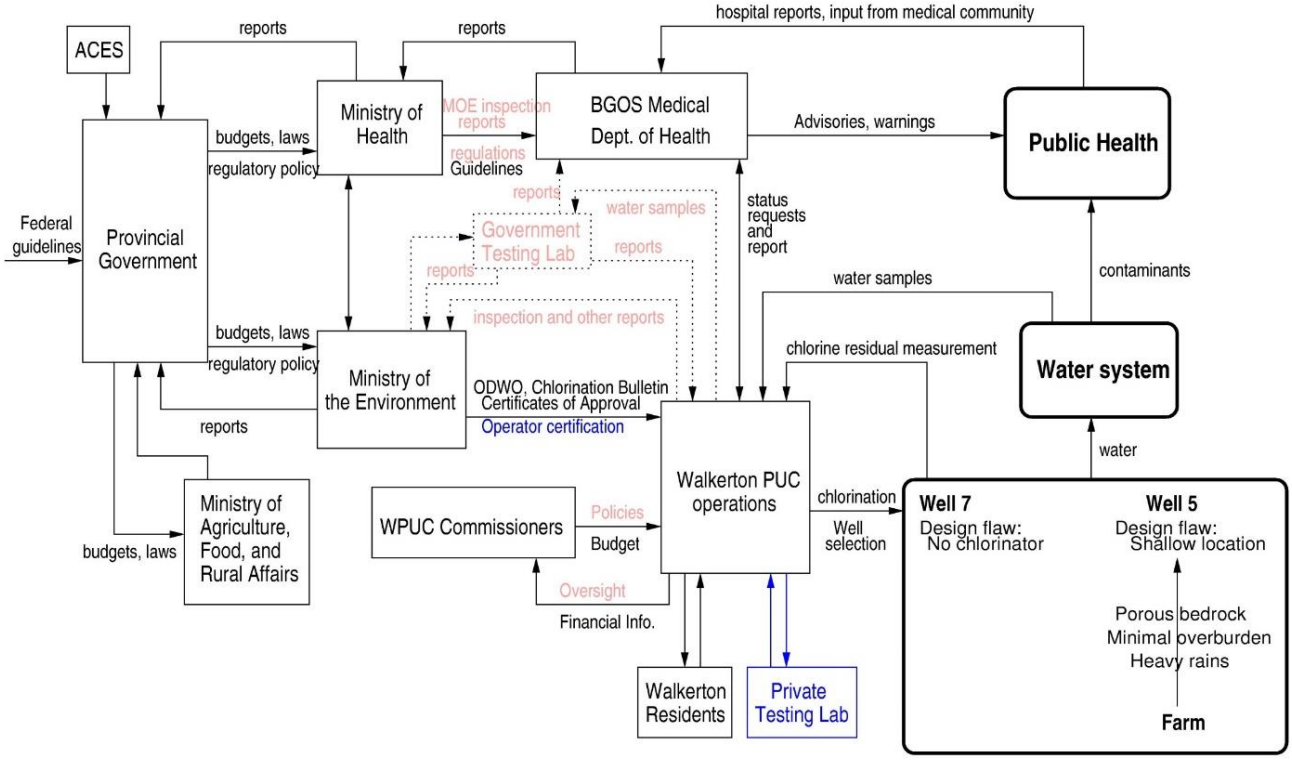



**Figure 21**: The control structure that existed at the time of the water contamination events.

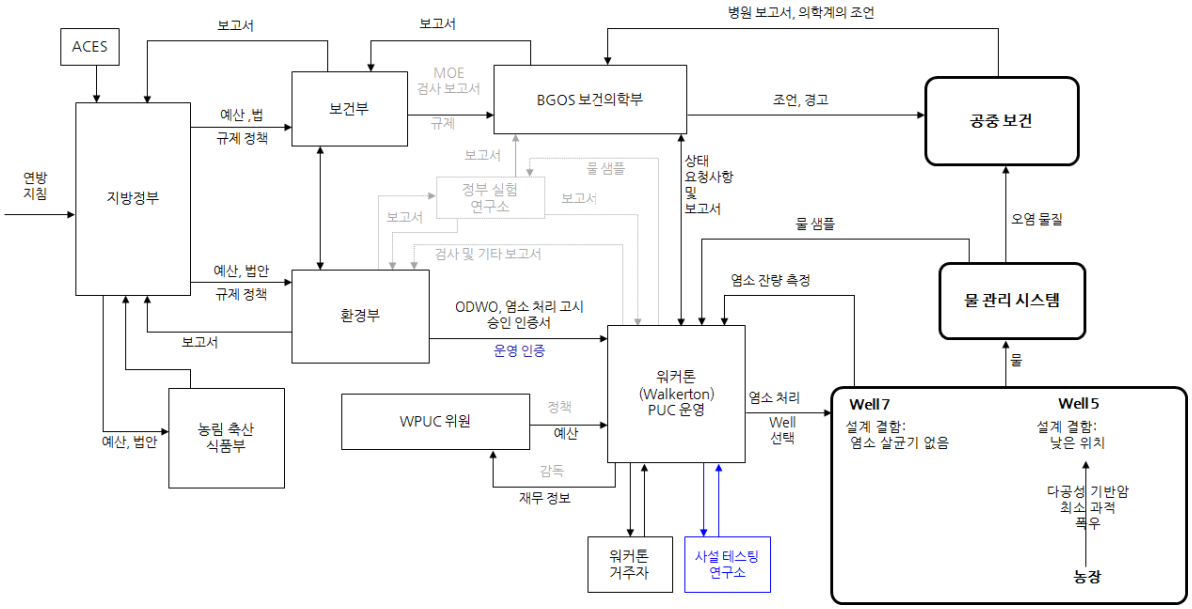



그림 21 : 수질 오염 이벤트 당시의 컨트롤 스트럭처

# Chapter 5: Using CAST for Workplace and Social Accidents

The examples so far in this handbook have involved traditional technical (engineered) systems plus the social systems that support them. CAST, however, can be used in less traditional applications. In this chapter, an example is provided of its use in workplace safety and also in situations where the hazards primarily involve social systems.

## Workplace Safety

As the example in this section demonstrates, there is no difference in the way that CAST is used for workplace safety compared to other types of systems. The example was a real accident, but unimportant details have been omitted for confidentiality reasons. Unlike the other examples in this handbook, there was no public investigation of the events.

The accident occurred in a manufacturing plant where large products were being assembled. A part was not ready at the time it should have been and had to be installed later in the assembly process. To accomplish the goal, part of the structure of the product needed to be disassembled so the new part could be inserted. Scaffolding was needed to perform the disassembly and the scaffolding was set up by the first shift. In the second shift, a four-man team performed a pre-task analysis and devised a plan to remove part of the structure to get to the space where the new part was to be inserted.

When the plan was executed, it was quickly discovered that the product could not be disassembled because the scaffolding blocked the removal of the outside structure. The four-man team decided to remove some of the center planks of the scaffolding to make the necessary room.

The team disassembled the structure and started moving it toward the scissor lift that was positioned at the opposite end of the scaffolding. While moving the structural part, a mechanic fell through the hole in the scaffolding, sustaining a serious injury involving multiple broken ribs.

A standard workplace injury analysis was performed by the company with the following conclusions taken directly from the report written by their accident investigation team:

**Direct Cause**: Employee fell from a height.

**Contributing Causes**:

- Lack of experience performing this work (it was out of the usual sequence of activities).
- Workers had no knowledge that there was a shop aid used for this type of job.
- The team did not perceive an out of ordinary risk in performing this job and did not ask for help.

**Root Cause**: Floor boards removed from scaffolding

**Near-Term Corrective Actions (Recommendations):**

- Create an alert to communicate that floorboards cannot be removed from scaffolding i.e., tell workers that it is very important not to remove floorboards from scaffolding.
- Ensure all floorboards in the factory are secured. [In the CAST analysis it will be seen that there are safety reasons for not securing the floorboards.]

**Longer-Term Corrective Actions:**

- Add tool information to job instructions for out-of-sequence work.
- Reset level of acceptable risk using this and other examples [*What does this mean?*]
- During daily crew kickoff meetings, discuss potential hazards and ensure safe work practices for the assigned tasks of the day. Move away from talking about generic safety

# 5장: 작업장 및 사회적 사고에 CAST 활용

지금까지 본 핸드북의 사례에는 전통적인 기술 시스템과 이를 지원하는 사회적 시스템이 포함되었다. 그러나 CAST는 그 밖의 응용분야에서도 사용될 수 있다. 이 장에서는 작업장 안전에서 CAST의 사용 그리고 주로 사회적 시스템과 관련된 위험 상황에서의 CAST 사용 사례를 소개한다.

## 작업장 안전(Workplace Safety)

본 섹션의 사례에서 알 수 있겠지만 CAST가 작업장 안전에 적용되는 방식은 다른 유형의 시스템에 적용되는 방식과 별 차이가 없다. 제시된 사례는 실제 발생한 사고였지만 기밀 유지를 이유로 일부 사항들은 생략되었다. 이 핸드북의 다른 사례와는 달리 그 이벤트에 대한 공개 조사는 없었다.

사고는 대형 제품들이 조립되고 있는 제조 플랜트에서 발생했다. 당시에 삽입되었어야 했던 부품이 준비되지 않아서 나중에 조립 공정에서 설치해야 했다. 작업 목표를 달성하기 위해 제품 구조의 일부를 분해하여 새로운 부품을 삽입할 수 있도록 해야 했다. 분해를 위해 비계(scaffolding)가 필요했고 첫 번째 교대자가 비계를 설치했다. 두 번째 교대에서는 4명의 팀이 사전 작업 분석을 통해 새로운 부품을 삽입할 공간을 확보하고자 구조물의 일부를 제거하는 계획을 수립했다.

계획을 이행하는 과정에서 비계가 외부 구조물의 제거를 방해하여 제품을 분해할 수 없다는 것을 알게 되었다. 4명의 팀은 필요한 공간을 확보하기 위해 비계의 중심 판자 일부를 제거하기로 했다.

그 팀은 구조물을 분해하여 비계의 반대쪽 끝에 위치한 시저 리프트(scicssor lift, 역주: 가위형의 고소작업대) 쪽으로 옮기기 시작했다. 그 구조물의 일부를 옮기는 동안 기계공이 비계 구멍으로 떨어져 갈비뼈가 여러 개 부러지는 중상을 입었다.

회사는 사고 조사팀이 작성한 보고서에서 다음과 같은 결론을 도출하여 표준 작업장 부상에 대해 분석하였다:

**직접적 원인:** 직원이 높은 곳에서 떨어졌다.

**기여 원인:**

- 이 작업(일반적인 작업 순서에 포함되지 않은 작업)을 수행한 경험이 부족했다.
- 작업자들은 이러한 종류의 업무에 사용되는 현장 작업지원(shop-aid)이 있다는 사실을 알지 못했다.
- 팀은 이 작업을 수행하는 데 있어 일상적 리스크를 감지하지 못했고 도움을 요청하지 않았다.

**근본적 원인:** 바닥판이 비계에서 제거되었다.

**단기 시정조치(권고사항):**

- 바닥판을 비계에서 제거해서는 안 된다는 경고문을 작성한다. 즉, 작업자에게 바닥판을 비계에서 제거하지 않는 것이 매우 중요하다고 전달한다.
- 플랜트의 모든 바닥판이 고정되어 있는지 확인해야 한다. [CAST 분석에서는 바닥판을 고정하지 <u>않는</u> 안전상의 이유가 있음을 알 수 있을 것이다.]

**장기적 시정조치:**

- 정해진 순서를 벗어난 작업에 대한 지침에 도구 정보를 추가한다.
- 이 사례 및 다른 사례를 통해 수용 가능한 리스크 수준을 재설정한다. [*이것은 무엇을 의미하는가?*]
- 일일 작업자 킥오프 미팅에서 잠재적 위험에 대해 논의하고 하루에 할당 작업에 대해 안전한 작업이 되도록 보장한다. 일반적인 안전 주제에 대한 논의에 국한하지 않는다. [*사후*

topics. [*It seems that only with hindsight bias would someone think to tell the crew not to remove floorboards from scaffolding. If everything that could possibly be done wrong was covered in the briefing, such meetings would take all day*.]

During the investigation, the analysis was at the level of asking and answering questions like

Question: "What did the employee do wrong? Answer: "Stepped in a hole."

Question: "What were the possible causes?" Answer: "Lack of situation awareness. Made a mistake."

The causes were derived in this instance by using something called a Reality Chart, which appears to be simply a fault tree with a misleading name. There is no such thing as objective "reality" but only reality as seen by each individual—which will usually be different for each viewer of or participant in an activity. That "reality" may be biased by the assumptions and prejudices of those doing the analysis. It may also be incomplete. Labeling something as "reality" is simply a misleading sales tool.

In this case, "lack of situation awareness" is a technical term that means "the person did not know the hole was there when he stepped in it." That is pretty obvious and not helpful. Why would anyone purposely step in a hole? It also is probably wrong. The worker did know about the hole. So, we still do not know why he stepped in it. One guess is that the large structural part being moved involved four people holding different sections. The worker that fell may have been forced into stepping into the hole by the movement of the part by the other workers. Note that even knowing more about why the worker stepped in the hole, in this case, does not provide much guidance in preventing this accident. The second reason given, i.e., "made a mistake," is even less useful.

One thing to note is that, as is usually the case, the accident report focused on the victim and the lowest level workers directly involved with the job being performed.

Lest the reader is unfamiliar with workplace injury causal analysis and thinks this example is a particularly bad one, be assured that it is not atypical. The company involved is very large, produces highly complex systems, and the process used to analyze this accident followed their standard written procedures and the process used in many, if not most, companies.

The corrective actions (recommendations) do not seem unreasonable until one compares them with those created by CAST. Note that allowing floorboards to be removed is a requirement to accomplish other safety and manufacturing goals so the consequences may conflict with other goals and therefore is likely to be ignored, particularly over time. Adding tool requirements for specific jobs in the factory certainly seems like a good idea (and surprising that it is not already done) but the other long-term corrective actions seem less useful or realistic. And, again, everything comes down to the workers following written directions, some of which may be unsafe.

*CAST Analysis of Scaffolding Accident*:

Because so little information was contained in the official accident report, the CAST analysis will necessarily be filled mostly with questions that needed to be answered at the time. But here is an outline of the most basic system components and CAST-generated questions:

*확신 편향으로 작업자들에게 비계에서 바닥판을 제거하지 말라고 이야기 했어야 한다고 생각할지 모른다. 그런데 만약 브리핑에서 잘못될 가능성 있는 모든 사안들을 다룬다면 회의가 하루 종일 걸릴 것이다.*]

조사 과정에서 분석은 다음과 같은 질문 및 답변 수준으로 이루어졌다.

질문: "직원이 무엇을 잘못했는가?" 답변: "구멍에 빠졌다."

질문: "가능한 원인은 무엇인가?" 답변: "상황 인식이 부족했다. 실수했다."

이 사례에서 현실 차트(Reality Chart)라는 것을 사용하여 원인을 도출하였다. 현실 차트는 이름에 오해의 소지가 있을 수 있지만 폴트 트리(fault tree) 형태를 띤다. 객관적인 "현실" 같은 것은 없으며 각각의 개인이 보는 현실만이 존재한다 — 이것은 대개 활동 관찰자나 참여자에 따라 다를 것이다. 그 "현실"은 분석을 수행하는 사람들의 가정과 편견에 의해 편향될 수 있다. 그것은 또한 완전하지 않을 수도 있다. 어떤 것을 "현실"이라고 명명하는 것은 단순히 오해를 불러일으키는 요인이다.

이 사례에서 "상황 인식 부족(lack of situation awareness)" 이라는 기술 용어는 "그가 빠졌을 때 그는 구멍이 있는 것을 몰랐다"는 것을 의미한다. 이것은 너무 뻔한 내용으로 문제해결에 도움이 되지 않는다. 어느 누가 일부러 구멍에 빠지겠는가? 아마도 잘못되었을 것이다. 그 작업자는 그 구멍에 대해 알고 있었을 것이다. 때문에 여전히 그가 구멍에 왜 빠졌는지 알지 못한다. 한 가지 추측으로는 4명의 작업자가 커다란 구조물의 서로 다른 부분을 잡고 이동시키는 것과 관련이 있을 것이다. 다른 작업자들이 발판의 일부를 이동시키는 바람에 그 작업자가 구멍으로 어쩔 수 없이 빠졌을 수도 있다. 이 경우 작업자가 왜 구멍에 빠졌는지에 대한 이유를 더 알게 되어도 이러한 사고를 방지하는 데 더 많은 지침을 주지는 못한다는 점에 유의해야 한다. 두 번째 이유, 즉, "실수했다"는 전혀 도움이 되지 않는다.

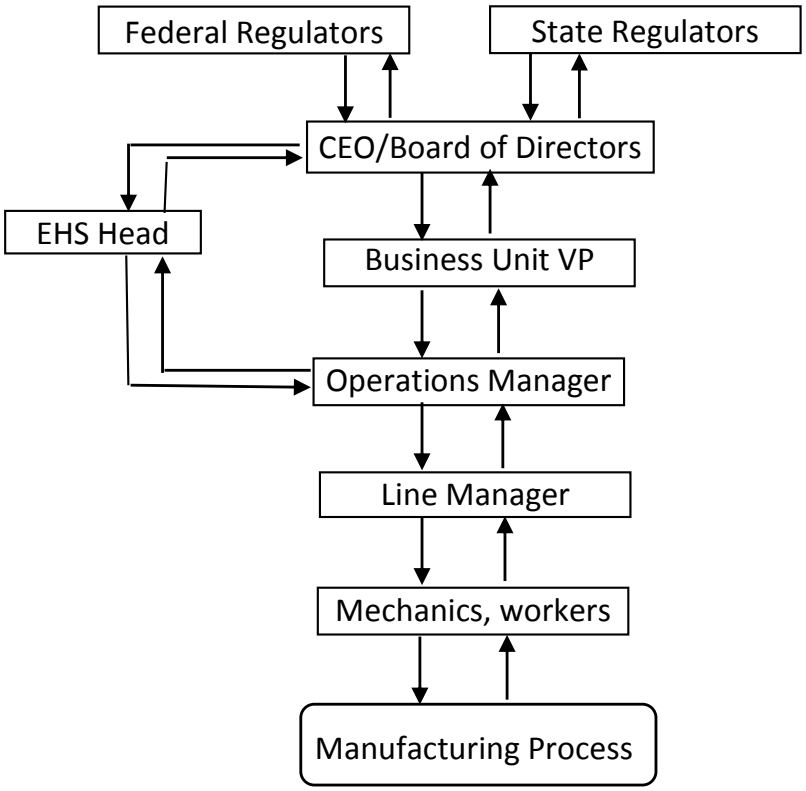
한 가지 주목할 점은, 사고 보고서가 보통의 경우와 같이 피해자와 수행 중인 업무에 직접적으로 연관된 최하위급 작업자에게 초점을 맞췄다는 것이다.

독자가 작업장 부상 사고의 원인 분석에 익숙하지 않고 이 사례가 특히 좋지 않은 예라고 생각할까봐 본 사례가 이례적인 것이 아님을 말해 둔다. 이 사례에서 회사는 매우 크고 매우 복잡한 시스템을 생산한다. 이 사고를 분석하는 데 사용된 프로세스는 그 회사의 표준 서면 절차서와 프로세스를 따랐고, 그 서면 절차서와 프로세스는 대부분은 아니지만 많은 회사에서 사용되는 것이었다.

시정조치(권고사항)는 CAST를 통해 생성한 것과 비교하기 전에는 그렇게 불합리해 보이지 않는다. 바닥판을 제거하도록 하는 것은 다른 안전 및 제조 목표를 위한 요구사항이기 때문에 그 요구사항의 결과가 다른 목표와 상충될 수 있고 특히 시간이 지남에 따라 이 요구사항은 무시될 수 있다는 점에 유의해야 한다. 플랜트에서 특정 작업을 위한 도구 요구사항을 추가하는 것은 확실히 좋은 아이디어인 것처럼 보이지만(아직 수행되지 않은 사실이 놀랍다) 다른 장기적 시정조치는 유용하지 못하거나 다소 현실성이 떨어지는 것처럼 보인다. 그리고 다시 말하지만 모든 것이 서면 지시에 따라 작업자들에게 전달되는데 그 중 일부는 안전하지 않을 수도 있다.

### *비계 사고의 CAST 분석:*

공식 사고 보고서에 포함된 정보가 너무 적기 때문에 필연적으로 CAST 분석은 대부분 당시 답변되었어야 하는 질문들로 채워질 것이다. 그렇긴 하지만 여기에 가장 기본적인 시스템 컴포넌트와 CAST가 만든 질문의 개요를 보여주고자 한다:




**Physical:**

Failures: none

Unsafe interactions: Worker fell through a hole in scaffolding

**Workers on First Shift**:

Responsibilities:

- Follow requests of their supervisor
- Follow documented standard procedures

Contribution to accident:

- Set up wrong type of scaffolding configuration

Mental Model Flaws:

- Did not know what job the scaffolding was for or did not understand the requirements of that job.

Context:

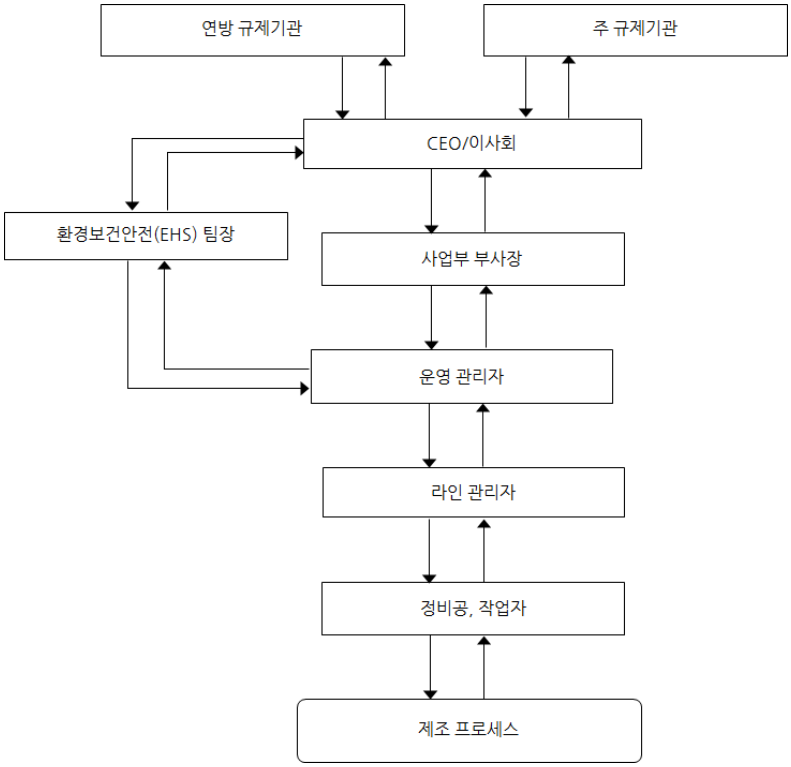
- Were they told to set up the scaffolding the way that they did?
- It was an out of sequence job that had not been completed at the time it should have been
- There was no documentation of the tools needed for the job or, alternatively, they may not have been told what the job was. [*What did they know about the job that needed the scaffolding and its requirements?]*

**First Shift Supervisor**:

Responsibilities:

- Provide job instructions to workers and ensure they have done the right job

Contribution to the accident:




**물리적:**

실패: 없음
안전하지 않은 상호작용: 작업자가 비계에 있는 구멍으로 떨어졌다.

**첫 번째 교대 작업자:**

책임:

- 감독자의 요청을 준수한다.
- 문서화된 표준 절차를 준수한다.

사고에 대한 기여:

- 잘못된 유형의 비계 구성을 설치하였다.

멘탈 모델 결함:

- 비계가 어떤 작업을 위한 것인지 몰랐거나 그 작업의 요구사항을 이해하지 못했다.

컨텍스트:

- 그들이 했던 방식대로 비계를 설치하라는 지시를 받았는가?
- 비계 설치는 정해진 순서를 벗어난 작업이었고 그 당시 완료되었어야 했는데 완료되지 않았다.
- 작업에 필요한 도구에 대한 문서가 없었거나 그 작업이 무엇인지 듣지 못했을 수도 있다.[*그들은 비계와 그 요구사항이 필요한 작업에 대해 무엇을 알고 있었는가?*]

**첫 번째 교대 감독자:**

책임:

- 작업자에게 작업 지침을 제공하고 맞게 수행했는지 확인한다:

- Either told workers to set up wrong type of scaffolding or did not check that right type was set up

Mental model flaws:

- *Did he know what job the scaffolding was needed for?*
- *Did he know there were special requirements for the scaffolding? If not, why not?*

Context:

- Out of sequence job that had not been completed at the time it should have been
- No documentation of tools needed for the job or they were not told what the job was.

**Second Shift Workers**:

Responsibilities:

- Perform their jobs as taught
- Use standard practices and tools called out in job instructions

Contribution to accident:

- Used unsafe scaffolding (removed the floor boards)
- *Did they check the jury rigging with their supervisor before they did it?*

Mental Model Flaws:

- Did not know there was scaffolding that should have been used for this job
- Did not know that they should not remove scaffolding to jury rig the tools they had been provided for the job.

Context:

- Unsafe scaffolding was set up for them to use that did not allow them to do the job they were told to do
- Correct tools were not documented
- *What experience did they have in doing this job? Was it the first time they had done it*? *If it was the first time, why were they unsupervised*?
- The reason for allowing scaffolding (floor boards) to be removed is that using wire or other materials to prevent scaffolding from being disassembled avoids the potential for FOD (foreign object debris), which is a serious hazard for these products.
- The culture in this company, which is documented in company policy, is that the highest priority is for workers to find a way to accomplish their goals without losing time in waiting for direction in how to do so from others. They are encouraged to find a way to get around problems without asking for instructions or help from others.

**Supervisor on Second Shift**:

Responsibilities:

- Ensure workers are using the proper and safe tools for job
- Ensure workers are aware of hazards, especially when doing out of sequence work

Contribution to accident:

- Allowed the use of unsafe scaffolding
- Did not properly supervise this out of sequence work

Mental model flaws:

- *Did he know the potential hazards?*
- *Did he know there was scaffolding that was designed for this type job? If not, why not?*

사고에 대한 기여:

- 작업자에게 잘못된 유형의 비계를 설치하라고 지시하거나 맞는 유형이 설치되었는지 확인하지 않았다.

멘탈 모델 결함:

- 그는 비계 제작이 어떤 일을 위해 필요했는지 알고 있었는가?
- 그는 비계를 위한 특별한 요구사항이 있다는 것을 알고 있었는가? 알지 못했다면 왜 그러했는가?

컨텍스트:

- 정해진 순서를 벗어난 작업이 그 당시에 완료되었어야 했으나 완료되지 않았다.
- 작업에 필요한 도구에 대한 문서가 없거나 해당 작업에 대한 설명을 듣지 못했다.

**두 번째 교대 작업자:**

책임:

- 배운대로 작업을 수행한다.
- 작업 지침서에 명시된 표준 작업 방식 및 도구 사용

사고에 대한 기여:

- (바닥판을 제거한) 안전하지 않은 비계 사용
- *그들은 작업 수행 전에 그들의 감독자와 같이 임시 조작을 점검했는가?*

멘탈 모델 결함:

- 이 작업에 사용되었어야 할 비계가 있다는 사실을 몰랐다.
- 작업을 위해 제공된 도구를 임시방편으로 사용하기 위해 비계를 제거하면 안 된다는 사실을 몰랐다.

컨텍스트:

- 안전하지 않은 비계를 설치하여 지시받은 작업을 수행할 수 없도록 하였다.
- 올바른 도구에 대한 정보가 문서화되지 않았다.
- *그들이 이 일과 관련된 어떤 경험이 있었는가? 그들이 그 작업을 한 것이 처음이었는가? 처음이었다면 그들은 왜 감독을 받지 않았는가?*
- 비계(바닥판)를 제거하도록 허용하는 이유는 와이어나 다른 재료를 사용하여 비계가 분해되는 것을 방지하면 이물질로 인한 피해(FOD, Foreign Object Debris)의 가능성을 피할 수 있기 때문이다. FOD는 이러한 제품에서 심각한 위험 요인이다.
- 회사 정책에 기록된 이 회사의 문화는 작업자들이 다른 사람들로부터의 지시를 기다리는 데 시간을 낭비하지 않고 목표를 달성할 수 있는 방법을 찾는 것을 최우선으로 하고 있었다. 즉, 다른 사람들에게 지시나 도움을 요청하지 않고 문제를 해결할 수 있는 방법을 찾는 것이 장려되었다.

**두 번째 교대 감독자:**

책임:

- 작업자가 작업을 위해 적절하고 안전한 도구를 사용하고 있는지 확인한다.
- 작업자가 정해진 순서를 벗어난 작업을 수행할 때 위험을 인지하고 있는지 확인한다.

사고에 대한 기여:

- 안전하지 않은 비계를 사용하도록 했다.
- 정해진 순서를 벗어난 작업에 대한 감독을 제대로 하지 않았다.

- *Did he know the workers had removed the floor boards?*
- *Did he check that proper scaffolding had been set up by prior shift?*

Context:

- Proper tools were not documented
- Out of sequence work is common in the factory

It is not possible to provide, after the fact, a detailed and useful CAST analysis of the upper levels of control in this accident because of the lack of information included in the accident report. There are, however, some intriguing unexplained statements in the accident report. For example, "The meeting with [company providing the out-of-sequence part] employees did not occur as planned." This statement was used in the explanation for why the wrong scaffolding was used. *Was there a meeting planned about how to fix the factory omission? Why did it not occur? Why did the work occur even though the meeting to plan how to do it was delayed?*

There are lots of questions that need to be answered to complete a CAST analysis and understand the cause of this accident, including:

- *Why were the workers doing a job for which they had no experience and without oversight from someone who did?*
- *Why did they not know about proper job aids, beyond the lack of documentation? What type of training is provided with respect to such jobs?*
- *Who has the responsibility to ensure that the right equipment is available and used? The immediate supervisor? Higher-level controllers?*
- *Why did the workers not ask for advice when the scaffolding design prevented them from doing their job? The answer here is probably related to the company culture.*
- *Who provides oversight for out-of-sequence work?*
- *Who evaluates the hazards of out-of-sequence work?*
- *Who is responsible for documenting what tools are needed for specific jobs and ensuring that workers know what these are? Why is it not standard practice to call out the tools to be used?*
- *How are out-of-sequence job steps and tools explained to employees?*
- *It appears that workers are used to jury-rigging solutions with no inputs from others. Is that true? How often does that occur? Why has nobody stopped this practice in the past? Is it expected by management?*
- *Why was the blame for not understanding the risks involved placed on the lowest-level workers and not their supervisors?*
- *Why was incorrect scaffolding constructed in the first place?*
- *Why was the part not inserted when it was originally supposed to be?*
- *There was a meeting scheduled about how to accomplish the work that had been canceled. Why was it never held? Why didn't the work wait until it could be held?*

멘탈 모델 결함:

- *잠재적 위험을 알고 있었는가?*
- *그는 이 유형의 작업을 위해 설계된 비계가 있다는 것을 알고 있었는가? 알지 못했다면 왜 인가?*
- *그는 작업자들이 바닥판을 제거했다는 것을 알고 있었는가?*
- *이전 교대조가 비계 설치를 제대로 했는지 확인했는가?*

컨텍스트:

- 적절한 도구에 대한 정보가 문서화되지 않음
- 플랜트에서 정해진 순서를 벗어난 작업이 흔히 발생한다.

사고 보고서에 포함된 정보가 부족하기 때문에 사후에 이 사고에 대한 상위 수준 컨트롤의 상세하고 유용한 CAST 분석을 제공하는 것은 불가능하다. 그러나 사고 보고서에는 설명할 수 없는 흥미로운 몇 가지 내용들이 있다. 예를 들어 "[작업 순서를 바꾸게 한 부품 납품 회사의] 직원과의 회의가 계획대로 진행되지 않았다." 이 내용은 잘못된 비계가 사용된 이유를 설명하는 데 사용되었다. *누락 사항을 어떻게 해결할 것인지에 대한 회의가 계획되어 있었는가? 왜 그 회의가 이루어지지 않았는가? 작업 방법을 계획하는 회의가 연기되었는데도 왜 그 작업이 수행되었는가?*

CAST 분석을 완료하고 이 사고의 원인을 파악하기 위해서 답변되어야 할 많은 질문들이 있다.

- *경험이 없는 작업자들이 누군가의 감독도 없이 작업을 수행한 이유는 무엇인가?*
- *그들이 서류상의 부족함을 채울 적절한 업무 지원책(job aids)에 대해 알지 못했는가? 그러한 업무와 관련하여 어떤 유형의 훈련이 제공되었는가?*
- *장비가 가용하고 사용될 수 있도록 하는 책임은 누구에게 있는가? 직속상관에게 있는가? 더 높은 수준의 컨트롤러에게 있는가?*
- *비계 설계로 일을 할 수 없게 된 작업자는 왜 조언을 구하지 않았는가? 여기에서의 답변은 아마도 회사 문화와 관련이 있을 것이다.*
- *정해진 순서를 벗어난 작업을 누가 감독하는가?*
- *정해진 순서를 벗어난 작업의 위험은 누가 평가하는가?*
- *특정 작업에 필요한 도구가 무엇인지 문서화하고 작업자가 이러한 도구를 알고 있는지 확인할 책임을 가지고 있는 사람이 누구인가? 사용할 도구를 명시하는 것이 표준 업무가 아닌 이유는 무엇인가?*
- *정해진 순서를 벗어난 작업의 단계와 도구들은 직원에게 어떻게 설명되고 있는가?*
- *작업자들은 다른 사람들의 의견 없이 임시방편으로 해결하는 데 익숙한 것으로 보인다. 사실인가? 얼마나 자주 그런 일이 일어나는가? 왜 아무도 과거의 이런 관행을 멈추지 않았는가? 경영진이 기대하고 있던 것인가?*
- *관련 리스크를 이해하지 못한 책임이 감독자가 아닌 최하위 직급의 작업자에게 있는 이유는 무엇인가?*
- *애초에 잘못된 비계가 만들어진 이유는 무엇인가?*
- *부품이 원래 삽입되기로 한 시점에 삽입되지 않은 이유는 무엇인가?*
- *취소된 작업을 어떻게 완수할 것인가에 대한 회의가 예정되어 있었다. 그 회의가 왜 열리지 않았는가? 회의를 할 수 있을 때까지 그 작업을 보류하지 않은 이유는 무엇인가?*

- *Did higher-level management know about these practices? If so, why was nothing done about it before an injury occurred? If not, why not? Were there no performance audits or feedback to oversee how work was being accomplished in the factory?*
- *Out-of-sequence work was common and low-level supervisors worried about injuries resulting from it but they were provided with no assistance in dealing with it. Why not?*

Answering these questions and additional ones that arose in the process is likely to generate more recommendations than "Tell workers not to remove floorboards from scaffolding." Here are some preliminary recommendations, without completing a CAST analysis:

- Do not allow workers to do any job without someone supervising it who is familiar with the tools that should be used for it and without being given proper instructions.
- Control the safety of out of sequence work much better than is currently done.
- Reduce the incidence of out-of-sequence work. While it probably cannot be totally eliminated, the occurrence arises in problems in the supply chain that need to be tackled.
- Plan contingency actions for out of sequence work and make sure proper tools are available. At the least, someone should be supervising this type of work.
- Document the tools, including scaffolding, that should be used for every type of job, not just this one.
- Provide better feedback and performance auditing of how hazardous activities are being performed and how the hazards are controlled.
- Perform better workplace hazard analysis and control hazards that are identified.

One of the things I learned from studying workplace training at this company is that workers are expected to identify the hazards of their jobs themselves and to take steps to mitigate them. Surprisingly, I have found this same expectation at other companies. One even asked workers to do a human factors analysis of their own jobs. These are people who mostly do not have a college education and are not qualified to accomplish these tasks. Where are the safety professionals who should be doing these things? Making the workers totally responsible for their own safety, of course, does provide a convenient scapegoat when accidents occur.

CAST can easily be applied to workplace accidents without significant changes to the process.

## Using CAST for Analyzing Social Losses

Most of the CAST analyses we have done ourselves have involved complex and dangerous physical systems and processes. CAST, however, can also be used to analyze social processes and other types of losses. This section provides some examples we have done. Links to the complete CAST analyses as well as many others are provided Appendix A. Two examples are described here: pharmaceutical safety in the U.S. and the causes of the 2008 financial system meltdown.

### *Pharmaceutical Safety Example*

Vioxx (Rofecoxib) was a prescription pain management drug primarily used by patients suffering from osteoarthritis. It was approved by the Food and Drug Administration (FDA) in May 1999. While on the market, it was one of the major sources of revenue for Merck, estimated to represent 11% of Merck's

- *최상위 경영진이 이러한 관행에 대해 알고 있었는가? 만약 그렇다면 부상이 발생하기 전에 아무 조치도 취하지 않은 이유는 무엇인가? 그러한 관행을 몰랐다면 왜 몰랐는가? 플랜트에서 작업이 어떻게 완수되고 있는지 감독할 성능 감사 또는 피드백이 없었는가?*
- *정해진 순서를 벗어난 작업을 하는 것이 흔한 일이었고 하위 수준 감독자는 그로 인한 부상에 대해 우려했지만 그에 대한 지원은 받지 못했다. 왜 그러했는가?*

이러한 질문들과 프로세스에서 발생한 추가 질문에 답변하면 "비계에서 바닥판을 제거하지 말라고 작업자들에게 말한다."라는 권고사항 보다 더 많은 권고사항을 생성할 수 있다. 다음은 CAST 분석을 완료하지 않은 상태에서 생성해 본 예비(preliminary) 권고사항이다.

- 사용해야 하는 도구에 익숙한 감독자의 감독 및 적절한 지침이 없다면 작업자가 어떠한 작업도 하지 못하게 한다.
- 정해진 순서를 벗어난 작업의 안전은 기존에 했던 작업들보다 훨씬 세심하게 컨트롤한다.
- 정해진 순서를 벗어난 작업의 발생률을 줄인다. 공급망에서 해결해야 하는 문제가 발생하므로 그러한 작업의 발생을 완전히 없앨 수는 없다.
- 정해진 순서를 벗어난 작업을 위한 비상 대책을 계획하고 적절한 도구가 가용한지 확인한다. 적어도 누군가는 이런 유형의 작업을 감독해야 한다.
- 이 작업뿐만 아니라 모든 유형의 작업에 사용해야 하는 도구(비계 포함)에 대해 문서화한다.
- 위험한 활동이 수행되는 방식과 위험이 컨트롤되는 방법에 대한 보다 나은 피드백과 성능 감사를 제공한다.
- 보다 나은 작업장 위험 분석을 수행하고 식별된 위험을 컨트롤한다.

이 회사에서 작업장 훈련에 대해 연구하면서 배운 것 중 하나는 작업자가 자신의 직무 위험을 스스로 파악하고 이를 완화하기 위한 조치를 취해야 한다는 것이다. 놀랍게도 필자는 다른 회사에서도 이와 같이 기대한다는 것을 발견했다. 어떤 회사는 작업자들에게 그들의 직무에 대한 인적 요인 분석을 요청하기도 했다. 작업자 대부분은 대학 교육을 받지 않았으며 이러한 일을 수행할 자격이 없는 사람들이다. 이러한 일을 해야 할 안전 전문가들은 어디에 있는가? 물론 작업자가 자신의 안전을 전적으로 책임지게 되면 사고가 발생할 때 그들을 희생양으로 삼기 용이하다.

CAST는 프로세스를 크게 변경하지 않고도 작업장 사고에 쉽게 적용할 수 있다.

## CAST를 활용한 사회적 손실 분석

우리가 수행한 대부분의 CAST 분석은 복잡하고 위험한 물리적 시스템 및 프로세스와 관련되어 있다. 그러나 CAST는 사회적 프로세스 및 기타 유형의 손실을 분석하는 데에도 사용할 수 있다. 이 섹션에서는 우리가 수행한 몇 가지 사례를 제시한다. 전체 CAST 분석 및 기타 여러 분석에 대한 링크는 부록 A에 제시한다. 여기서는 미국의 제약 안전성과 2008년 금융 시스템 붕괴의 원인에 대한 두 가지 사례가 여기에 설명한다.

### *제약 안전 사례*

바이옥스(Vioxx, 로페콕시브(Rofecoxib)계열)는 골관절염을 앓고 있는 환자가 주로 처방받아 사용하는 통증 관리 약물이었다. 그 약물은 1999년 5월 미국 식품 의약국(FDA)의 승인을 받았다. 또한 그

sales in 2003. In September 2004, after the U.S. drug safety control structure had allowed this dangerous drug to be left on the market for over five years, Merck voluntarily withdrew the drug because of safety concerns. According to an epidemiological study by an FDA scientist, Vioxx was associated with more than 27,000 heart attacks or deaths: "Vioxx may be the single greatest drug safety catastrophe in the history of this country or the history of the world."[23]

The losses in this example are identified as:

Losses ("Accidents"):

1. Patients get a drug treatment that negatively impacts their health, in this case fatal cardiovascular events such as heart attacks and strokes
2. Patients do not get the treatment they need.

Emphasis in this example is on the first loss, i.e., patients get a drug treatment that negatively impacts their health, because Vioxx, in the end, did not appear to have been more effective than normal over-the-counter pain medication so they could have gotten the treatment they needed.

Hazards: (common to all pharmaceutical products)

H1: The public is exposed to an unsafe drug

1. The drugs are released with a label that does not correctly specify the conditions for safe use of the drug
2. Approved drugs are found to be unsafe and appropriate responses are not taken (warnings, withdrawals from the market, etc.)
3. Patients are subjected to unacceptable risk during clinical trials

H2: Drugs are taken unsafely

1. The wrong drug for the indication is prescribed
2. The pharmacist provides incorrect medication
3. The drugs are taken in an unsafe combination
4. The drugs are not taken according to directions (dosage and timing)

H3: Patients do not get an effective treatment they require

1. Safe and effective drugs are not developed or are not approved for use
2. Safe and effective drugs are not affordable for those who need them
3. Unnecessary delays are introduced into development and marketing
4. Physicians do not prescribe needed drugs or patients have no access to those who could provide the drugs to them
5. Patients stop taking a prescribed drug due to perceived ineffectiveness or intolerable side effects.

The reader can see that some of the hazards conflict, making decision making about pharmaceuticals quite complicated and difficult.

These hazards can be translated into safety requirements and constraints:

[23] Testimony of David J. Graham, MD, MPH, November 18, 2004, U.S. Senate, 2004.

약물은 시중에 유통될 당시 머크社의 주요 수입원 중 하나였고 매출의 약 11% 정도를 차지하였다. 미국의 의약품 안전 컨트롤 스트럭처가 이 위험한 약물을 5년 이상 시중에 방치하였고 Merck社는 2004년 9월 안전에 대한 우려로 자발적으로 약물을 회수하였다. FDA 과학자의 역학 연구에 따르면 바이옥스는 27,000건 이상의 심장마비 또는 사망 사고와 관련되어 있다고 하였다: "바이옥스는 단일 약물로는 이 나라 역사뿐만 아니라 전 세계 역사상 가장 최악의 안전 참사일 것이다."[23]

이 사례에서의 손실은 다음과 같이 파악된다.

손실("사고"):
1. 환자가 건강에 부정적인 영향을 주는 약물 치료를 받게 되는 경우 심장마비나 뇌졸중과 같은 치명적인 심혈관 질환이 발생한다.
2. 환자가 필요한 치료를 받지 못한다.

이 사례에서 강조되는 것은 첫 번째 손실이다. 즉, 환자들이 건강에 부정적인 영향을 미치는 약물 치료를 받는 것이다. 왜냐하면, 바이옥스는 결국, 처방전 없이 살 수 있는 일반 진통제보다 더 효과적으로 보이지 않았기 때문이며 그들이 일반 진통제를 샀다면 그들이 원하는 치료를 받았을 수도 있었다.

위험원: (모든 의약품에 공통)

H1: 대중들은 안전하지 않은 약물에 노출되어 있다.
1. 약물의 안전한 사용 조건이 제대로 명시되지 않은 라벨을 부착한 채 약물이 출시된다.
2. 승인된 약물이 안전하지 않은 것으로 밝혀지고 그에 대한 적절한 대응(경고, 시장에서의 철수 등)을 하지 않는다.
3. 임상 시험 중 환자가 수용할 수 없는 리스크에 노출된다.

H2: 약물이 안전하지 않게 취급된다.
1. 명시된 약물이 아닌 잘못된 약물을 처방한다.
2. 약사가 잘못된 약물을 제공한다.
3. 안전하지 않은 조합으로 약물을 복용한다.
4. 지시(복용량 및 시기)에 따라 약물을 복용하지 않는다.

H3: 환자가 필요로 하는 효과적인 치료를 받지 못한다.
1. 안전하고 효과가 있는 약물이 개발되지 않았거나 사용 승인을 받지 못한다.
2. 안전하고 효과가 있는 약물이 그것을 필요로 하는 사람에게 제공되지 않는다.
3. 개발 및 마케팅이 불필요하게 지연된다.
4. 의사들이 필요한 약물을 처방하지 않거나, 환자들이 그들에게 약을 제공할 수 있는 사람들에게 접근할 수 없다.
5. 환자가 약물을 효과가 없다고 인식하거나 견딜 수 없는 부작용 때문에 처방된 약의 복용을 중단한다.

독자들은 몇 가지 위험요인이 상충되어 의약품에 대한 의사결정이 매우 복잡하고 어려워진다는 것을 알 수 있을 것이다.

이러한 위험은 다음과 같은 안전 요구사항과 제약사항으로 변환될 수 있다:

[23] Testimony of David J. Graham, MD, MPH, November 18, 2004, U.S. Senate, 2004.

Safety Requirements and Constraints for Pharmaceutical Products:

1. Pharmaceutical products are developed to enhance long-term health
    a. Continuous appropriate incentives exist to develop and market needed drugs
    b. New scientific knowledge and technology is developed to create new drugs
    c. New drugs are developed and manufactured only when the scientific and technical knowledge is available

2. Drugs on the market are adequately safe and effective
    a. Drugs are subjected to effective and timely safety testing
    b. New drugs are approved by the FDA based upon a validated and reproducible decision-making process
    c. Drug approval is not unnecessarily delayed
    d. The labels attached to drugs provide correct information about safety and efficacy
    e. Drugs are manufactured according to Good Manufacturing Practices
    f. Marketed drugs are monitored for known and unknown adverse events, side effects, and potential negative interactions
    g. Long term studies are conducted, even after the drug as been approved, to validate the FDA's approval decision (e.g., Phase IV studies) both on the long term and for subpopulations
    h. New information about potential safety risks is reviewed by an independent advisory board
    i. Marketed drugs found to be unsafe after they are approved are removed, recalled, restricted, or appropriate risk/benefit information is provided

3. Patients get and use the drugs they need for good health
    a. Drugs are obtainable by patients
    b. Accurate information is available to support decision-making about risks and benefits
    c. Patients get the best intervention reasonable for their health needs
    d. Patients get drugs with the required dosage and purity

4. Patients take the drugs in a safe and effective manner
    a. Patients get correct instructions about dosage and follow them
    b. Patients do not take unsafe combinations of drugs
    c. Patients are properly followed by a physician while they are being treated
    d. Patients are not subjected to unacceptable risk during clinical trials

The safety control structure we used has five main components (Figure 22): the FDA, Pharmaceutical companies, patients, academically-affiliated researchers, and the healthcare providers as well as a variety of others who play a role in drug safety (Congress, Journal editors, patient groups, etc.). The responsibilities of the controllers are described in the individual component CAST analyses. Only a few

의약품 안전 요구사항 및 제약사항:

1. 장기적인 건강 증진을 위해 의약품을 개발한다.
   a. 필요한 약물을 개발하고 판매하기 위해 지속적이고 적절한 인센티브를 제공한다.
   b. 새로운 약물을 만들기 위해 새로운 과학 지식과 기술을 개발한다.
   c. 과학적, 기술적 지식이 가용한 경우에만 새로운 약물을 개발 및 제조한다.

2. 시중에 유통되는 약물은 충분히 안전하고 효과가 있다.
   a. 약물에 대해 효과적이고 시기적절한 안전 테스트를 수행한다.
   b. 새로운 약물에 대해 검증되고 재현 가능한 의사결정 과정에 근거하여 FDA의 승인을 받는다.
   c. 약물 승인이 불필요하게 지연되지 않는다.
   d. 약물에 부착된 라벨에 안전성과 효능에 대한 정확한 정보를 제공한다.
   e. 우수 제조 관리 기준(Good Manufacturing Practices)에 따라 약물을 제조한다.
   f. 시판되는 약물에 대해서 알려져 있거나 알려지지 않은 부정적 이벤트, 부작용 및 잠재적으로 부정적인 상호작용에 대해 모니터링한다.
   g. 약물이 승인된 후에도 장기적 및 부분 모집단에 대한 FDA의 승인 결정(예: 4단계 연구)을 검증하기 위해 장기적인 연구를 수행한다.
   h. 독립 자문 위원회를 통해 잠재적 안전 리스크에 대한 새로운 정보를 검토한다.
   i. 승인 후 안전하지 않은 것으로 확인된 약물에 대해서는 제거, 회수, 제한하거나 적절한 리스크/효능에 대한 정보를 제공한다.

3. 환자는 건강을 위해 필요한 약물을 구하고 사용한다
   a. 환자는 약물을 구할 수 있다.
   b. 리스크 및 효능에 대한 의사결정을 지원하기 위해 정확한 정보를 이용할 수 있다.
   c. 환자는 그들의 건강에 합당한 최상의 중재처방을 받는다.
   d. 환자는 필요한 복용량 및 순도의 약물을 복용한다.

4. 환자는 안전하고 효과적인 방법으로 약물을 복용한다.
   a. 환자는 복용량에 대한 올바른 지시를 받고 이를 따른다.
   b. 환자는 안전하지 않은 약물 조합을 복용하지 않는다.
   c. 환자는 치료받는 동안 의사의 지시를 적절히 따라야 한다.
   d. 환자는 임상 시험 중 수용할 수 없는 리스크에 노출되지 않는다.

우리가 사용한 안전 컨트롤 스트럭처에는 5개의 주요 컴포넌트가 있다(그림 22): FDA, 제약회사, 환자, 학술연계 연구원(academically-affiliated researchers), 의료 제공자 및 약물 안전에 관여하는 다양한 요소(의회, 저널 편집자, 환자 그룹 등). 개별 컴포넌트에 대한 CAST 분석 내용에 컨트롤러의 책임이 설명되어 있으며, 여기에는 몇 가지 CAST 분석 사례만 제시한다. Matthieu Couturier가 수행한 전체 분석 결과는 부록 A에서 확인할 수 있다.

examples from the CAST analysis are presented here. The complete analysis by Matthieu Couturier can be found in Appendix A.

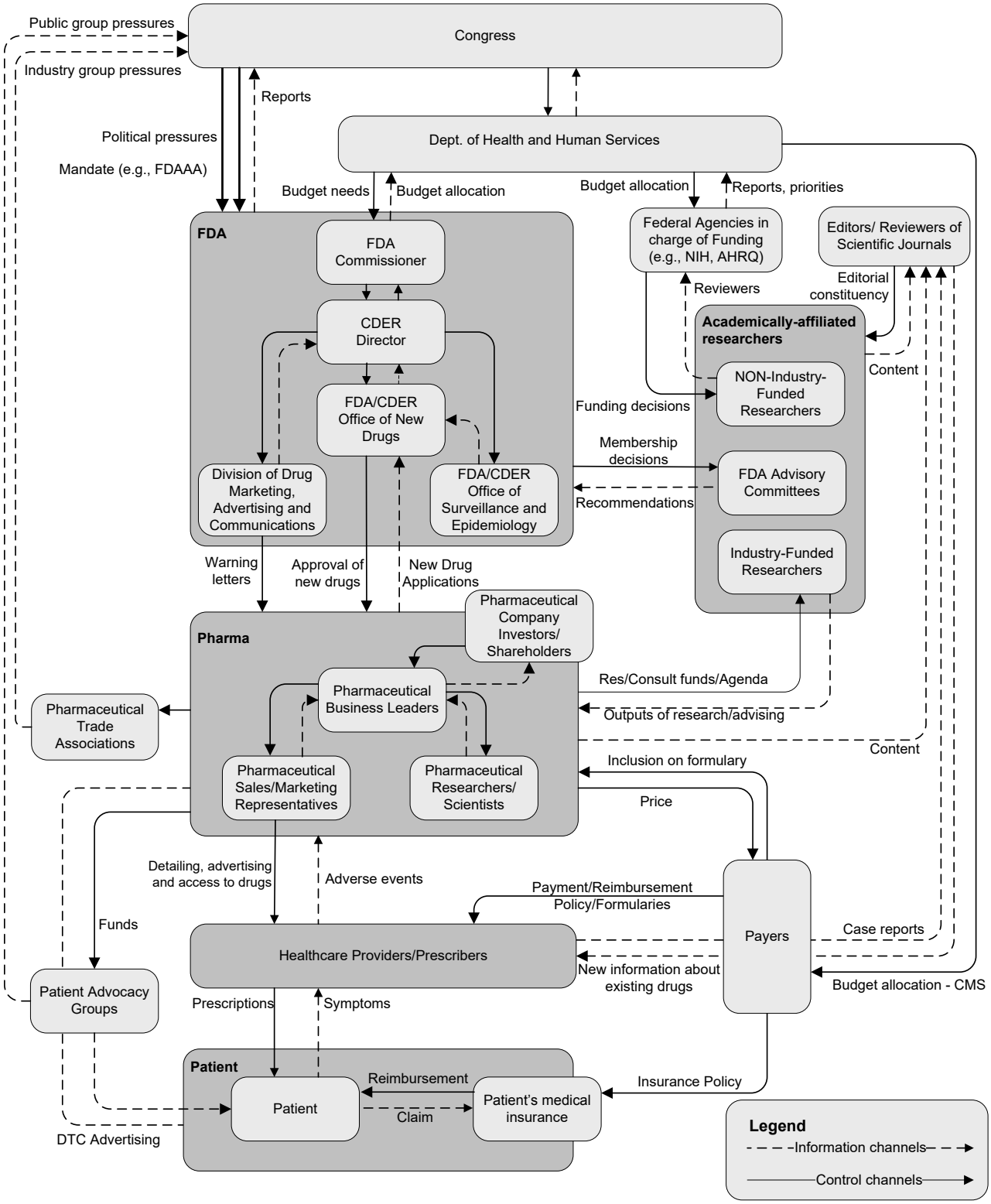



**Figure 22**: The pharmaceutical safety control structure in the U.S.

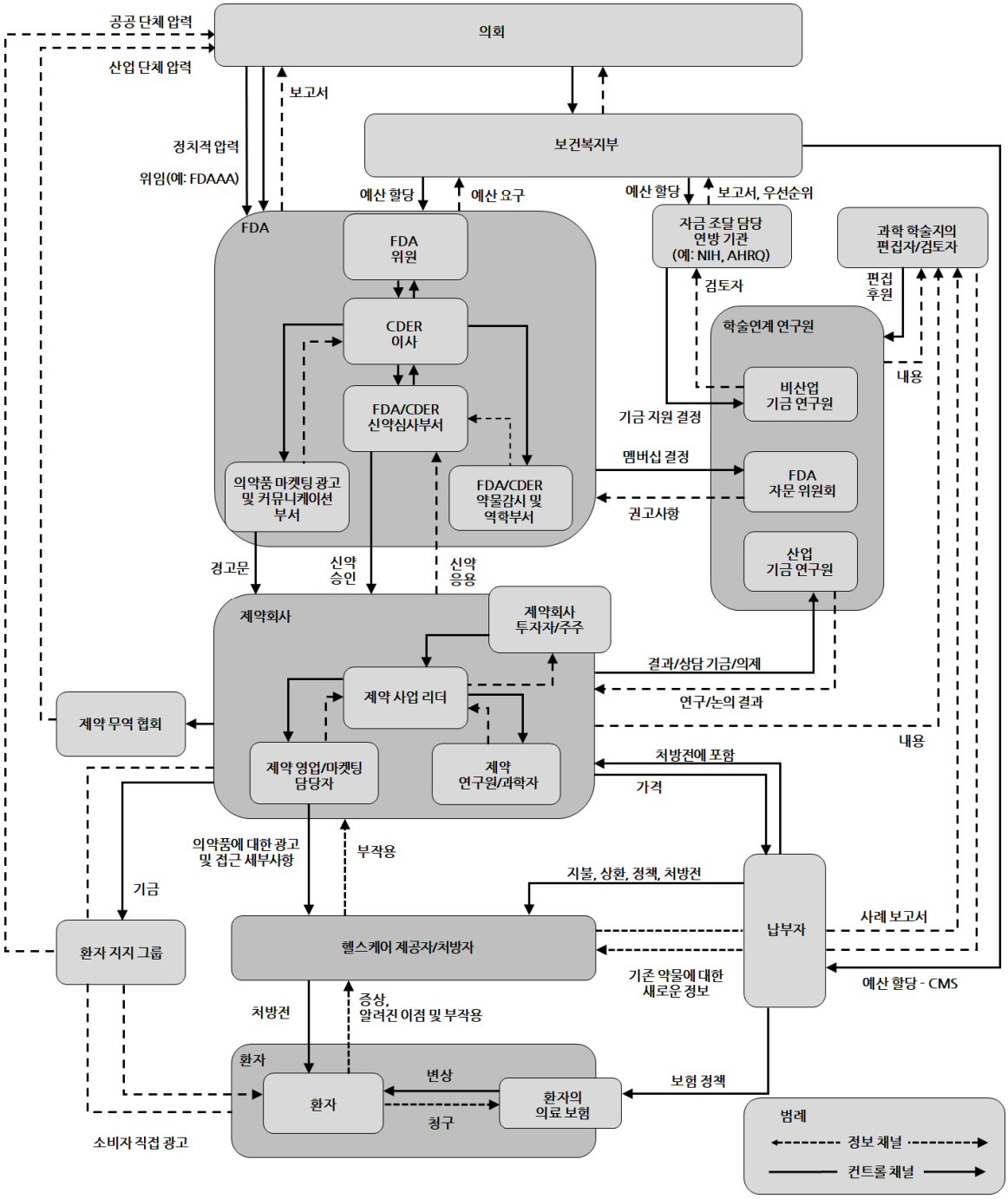



그림 22 : 미국의 제약(phamaceutical) 안전 컨트롤 스트럭처

## Patients

Responsibilities:

1. Accept limited responsibility for their own health and treatment (limited by what is practical).
2. Follow their physician's instructions and take drugs as prescribed.
3. Accede to doctor's superior knowledge when appropriate.
4. Go through a doctor to get a prescription for drugs like Vioxx.

Contribution to Losses:

1. Some patients pressured their doctor into prescribing Vioxx even if it was not necessarily the most appropriate treatment for their specific needs.

Mental Models:

1. Patients believed that the drug was safer than it really was.
2. Patients believe that newer, more expensive drugs are better than older, alternative treatments.

Context in Which Decisions Were Made:

1. Patients had limited information about the safety and effectiveness of Vioxx. Most of the information that they had came from Direct-To-Consumer (DTC) advertising, which provided a rosy picture of the efficacy of the drug along with glamorous and respected spokespersons (e.g., the famous ice skater Dorothy Hamill).
2. Patients have limited medical knowledge about both their disease and the medication they are taking and have to rely on their doctor's opinion and advice.
3. Vioxx was approved by the FDA which they assumed provided a "guarantee" of safety. It was apparently endorsed by the medical community in medical journals and tacitly endorsed by insurance companies (which are willing to reimburse the patients for the new treatments).
4. A large number of patients taking Vioxx should not have been taking the drug because they had very low risk of gastrointestinal problems and therefore should have been prescribed non-steroidal anti-inflammatory drugs (NSAIDs).

## 환자(Patients)

책임:

1. 자신의 건강과 치료를 위해 제한된 범위(실행 가능한 범위에서)의 책임을 진다.
2. 의사의 지시에 따라 처방된 대로 약물을 복용한다.
3. 의사의 전문 지식이 타당한 경우 수긍한다.
4. 바이옥스와 같은 약물의 처방전은 의사를 통해서만 받는다.

손실에 대한 원인:

1. 일부 환자들은 바이옥스가 그들에게 가장 적절한 치료법이 아닌 경우에도 의사에게 바이옥스를 처방해달라고 압박했다.

멘탈 모델:

1. 환자들은 약물이 실제보다 더 안전하다고 믿는다.
2. 환자들은 새롭고 더 비싼 약물이 오래된 대체 치료법보다 낫다고 믿는다.

의사결정이 이루어진 컨텍스트:

1. 환자는 바이옥스의 안전성과 효과에 대한 정보를 제한적으로 가지고 있었다. 그들이 얻은 대부분의 정보는 DTC(Direct-To-Consumer) 광고에서 비롯되었으며 이 광고에서는 매력적이고 존경받는 대변인(예: 유명한 아이스 스케이트 선수 도로시 해밀(Dorothy Hamill))이 약물의 효능에 대해 낙관적으로 표현했다.
2. 환자들은 자신의 질병과 복용 중인 약물에 대한 의학 지식을 제한적으로 가지고 있었으므로 의사의 의견과 조언에 의존해야 한다.
3. 바이옥스는 FDA에서 승인을 받았다. 이것은 안전에 대한 “최소한의 보장(guarantee)”을 부여함을 의미하였다. 의학계는 의학 저널에서 바이옥스에 대해 명백히 보증하였고 (새로운 치료법에 대해 환자들에게 보상해야 하는) 보험 회사가 암묵적으로 보증하였다.
4. 위장 질환과 관련된 리스크가 매우 낮은 많은 환자들은 바이옥스를 복용하지 않았어야 했으며 비스테로이드성 항염증제(NSAID)를 처방받았어야 했다.

## Healthcare Providers/Prescribers

Responsibilities:

1. Make treatment decisions based on the best interests of their patients.
2. Weigh the risks of treatment and non-treatment.
3. Prescribe drugs according to the limitations on the label.
4. Maintain an up-to-date mental model of the risk/benefit profile of the drugs they are prescribing.
5. Monitor symptoms of their patients under treatment for adverse events and negative interactions.
6. Report adverse events potentially linked to the use of the drugs being prescribed.

Contribution to Losses:

1. Doctors prescribed Vioxx, both on and off label, for patients for whom it was not indicated.

Mental Models:

1. Believed that new drugs are better than existing treatments.
2. Believed that information from pharmaceutical companies is accurate.
3. Did not understand the risk/benefit tradeoffs of Vioxx. In particular, they did not know about potential cardiovascular risks associated with the long-term use of the drug.
4. Believed that patients might go to another practitioner if Vioxx was not prescribed.

Context in Which Decisions Were Made:

1. Doctors mostly learn about new products from the drug companies themselves.
2. Doctors are notoriously busy and their time is limited for reading medical journals and keeping up with the latest treatments or with thoroughly discussing the benefits and risks of a treatment.
3. Doctors have limited access to unbiased information.
4. Studies of new drugs are typically done against placebos. Doctors are left without the information needed to decide which approved drug is a more appropriate treatment for a specific patient.
5. Doctors are part of the service industry and do not want to alienate their patients by not prescribing the drugs they request.
6. Vioxx label (from FDA) did not mention cardiovascular risks.

## 의료 서비스 제공자/처방자(Providers/Prescribers)

책임:

1. 환자의 최선의 이익(best interests)을 기반으로 치료 결정을 내린다.
2. 치료와 비치료의 리스크를 따져 본다.
3. 라벨에 있는 제한사항에 따라 약물을 처방한다.
4. 처방하고 있는 약물의 리스크/이익 프로필에 대한 최신 멘탈 모델을 유지한다.
5. 치료 중인 환자의 부작용과 부정적인 상호작용에 대한 증상을 모니터링 한다.
6. 처방되는 약물의 사용과 잠재적으로 관련된 부작용을 보고한다.

손실에 대한 기여:

1. 의사들은 바이옥스 처방에 해당되지 않는 환자들에게 라벨이 붙어있거나 붙어있지 않은 바이옥스를 처방했다.

멘탈 모델:

1. 신약이 기존 치료보다 낫다고 믿는다.
2. 제약회사의 정보가 정확하다고 믿는다.
3. 바이옥스의 리스크/이익의 트레이드오프를 이해하지 못했다. 특히, 약물의 장기적 사용과 관련된 잠재적인 심혈관 리스크에 대해 알지 못했다.
4. 바이옥스를 처방하지 않으면 환자들이 다른 의사에게 갈 수도 있다고 생각했다.

의사결정이 이루어진 컨텍스트:

1. 의사들은 대부분 제약회사로부터 새로운 약품에 대해 배운다.
2. 의사들은 매우 바쁘기 때문에 의료 저널을 읽거나, 최신 치료법 인지하거나, 치료의 이점 및 리스크를 심도있게 논의하는 시간이 제한되어 있다.
3. 의사들은 편향적이지 않은 정보에 대한 접근이 제한되어 있다.
4. 신약에 대한 연구는 일반적으로 플라세보(placebo, 속임약)에 대비를 이루어 수행된다. 의사들은 승인된 어떤 약물이 특정 환자에게 더 적절한 치료법인지 결정하기 위해 필요한 정보가 없다.
5. 의사들은 서비스 산업의 구성원이며 환자가 요구하는 약물을 처방하지 않아서 환자들을 떠나가는 것을 원치 않는다.
6. 바이옥스 라벨(FDA에서 받은)에는 심혈관 리스크가 언급되지 않는다.

## Merck

Responsibilities:

1. Ensure that patients are protected from avoidable risks:
   a. Provide safe and effective drugs.
   b. Test drugs for effectiveness.
   c. Properly label the drugs.
   d. Protect patients during clinical trials by properly monitoring the trial.
   e. Do not promote unsafe use of the drugs.
   f. Remove a drug from the market if it is no longer considered safe.
   g. Manufacture the drugs according to Good Manufacturing Practices.
2. Monitor drugs for safety:
   a. Run long-term post-approval studies as required by the FDA.
   b. Run new trials to test for potential safety hazards.
   c. Provide, maintain, and incentivize adverse-event reporting channels.
3. Give accurate and up-to-date information to doctors and the FDA about drug safety:
   a. Educate doctors.
   b. Provide all available information about the safety of the drug to the FDA.
   c. Inform the FDA of potential new safety issues in a timely manner.
4. Conduct or sponsor research that can be useful for the development of new drugs and treatments.

Contribution to Losses:

1. Merck did not run studies that might have found negative cardiovascular (CV) results. Company executives rejected doing a study of Vioxx's CV risks.
2. Merck's studies, and the results the firm published, inadequately represented the risk/benefit profile of the drug:
   a. The studies were motivated by marketing goals.
   b. If the results were published, they were typically released very late or only partially released.
   c. The results were biased to appear better than they were.
   d. Some of the studies that were run did not have an active Data and Safety Monitoring Board (DSMB) to monitor the clinical trials and protect the patients. The safety of the patients was solely in the hands of the Merck investigators.
3. Merck published and disseminated misleading information about the safety profile of Vioxx:
   a. Merck aggressively promoted drug usage with a task force trained to avoid CV questions.
   b. Merck used promotional activities and materials that were false, lacking in fair balance or otherwise misleading. The company continued to minimize unfavorable findings up to a month before withdrawing Vioxx.
   c. Merck published or promoted publication using guest authorship or ghostwriting; Merck employees' involvement in the writing process was often not mentioned and the financial ties of the main authors were not always disclosed.
   d. Merck created journals made to look like independent peer-reviewed journals. These journals were actually marketing compilations of articles promoting Vioxx and another drug made by Merck.

## 머크(Merck)

책임:

1. 피할 수 있는 리스크로부터 환자를 보호한다:
   a. 안전하고 효과적인 약물을 제공한다.
   b. 약물의 효능을 시험한다.
   c. 약물에 적절한 라벨을 부착한다.
   d. 임상시험 중 적절한 모니터링으로 환자를 보호한다.
   e. 안전하지 않은 약물의 사용을 독려하지 않는다.
   f. 약물이 더 이상 안전하지 않다고 간주되면 시장에서 해당 약물을 회수한다.
   g. 우수제조관리기준(Good Manufacturing Practices)에 따라 약물을 제조한다.
2. 안전을 위한 약물 모니터링:
   a. FDA의 요구에 따라 승인 후 장기적인 연구를 수행한다.
   b. 잠재적 안전 위험을 테스트하기 위해 새로운 시험을 수행한다.
   c. 부작용 보고 채널을 제공, 유지, 장려한다.
3. 의사와 FDA에게 약물 안전에 대한 정확한 그리고 최신의(up-to-date) 정보를 제공한다:
   a. 의사들을 교육한다.
   b. 약물의 안전성에 대한 모든 가용한 정보를 FDA에 제공한다.
   c. 새로운 잠재적 안전 문제를 FDA에 적시에 통보한다.
4. 신약 및 치료제 개발에 유용한 연구를 수행하거나 후원한다.

손실에 대한 기여:

1. 머크社는 부정적인 심혈관(CV) 결과를 발견할 수도 있었을 연구를 수행하지 않았다. 회사 경영진은 바이옥스의 CV 리스크에 대한 연구를 거부했다.
2. 머크社의 연구, 그리고 기업이 발표한 결과에 약물의 리스크/이익 프로파일이 부적절하게 표현되었다:
   a. 연구의 동기가 마케팅 목표였다.
   b. 결과가 발표된 경우 결과는 대개 아주 늦게 발표되거나 부분적으로만 발표되었다.
   c. 그 결과들은 실제보다 더 나아 보이도록 편향되었다.
   d. 수행한 일부 연구에는 임상시험을 모니터링하고 환자를 보호하기 위한 능동적 데이터 및 안전 모니터링 위원회(DSMB, Data and Safety Monitoring Board)가 없었다. 환자들의 안전은 오로지 머크社 연구원의 손에 달려 있었다.
3. 머크社는 바이옥스 안전 프로필에 대한 잘못된 정보를 발표하고 배포했다:
   a. 머크社는 심혈관 질문을 피하도록 훈련받은 TF(Task Force)와 함께 약물 사용을 적극적으로 홍보했다.
   b. 머크社는 허위, 공정성 부족 또는 오해의 소지가 있는 홍보 활동과 자료를 사용했다. 머크社는 바이옥스를 회수하기 한 달 전 까지 계속해서 불리한 자료들을 감추려고 했다.
   c. 머크社는 객원 저자 또는 대필을 사용하여 출판하거나 출판을 홍보했다; 머크社 직원들이 글쓰기 과정에 참여한 것은 거의 언급되지 않았고 주 저자의 재정적 관계가 항상 공개된 것은 아니었다.
   d. 머크社는 저널들을 만들었으며 독립적인 동료 검토(peer-review)를 수행한 저널처럼 보이게 했다. 이 저널들은 실제로 바이옥스와 머크社에서 만든 또 다른 의약품을 홍보하는

Mental Models

1. Merck originally believed that Vioxx did not cause any CV events.
2. Believed Vioxx had the potential to become a blockbuster drug and significant source of revenue if only Merck could effectively limit the publication of negative results and convince doctors to prescribe the drug despite potential CV risks.
3. Believed the company could protect its reputation by hiding negative results.
4. Believed it could convince doctors to prescribe the drug despite the potential CV risks.

Context*:*

1. Merck has a fiduciary duty to shareholders to provide a return on their investment and stakeholders demand a high return. Furthermore, drug company executives are partly paid in stock options.
2. Satisfactory financial results depended on Vioxx being a blockbuster.
    a. Vioxx was a major source of Merck's revenue and was extremely profitable.
    b. Vioxx faced fierce competition from Celebrex, which was approved by the FDA 5 months before it approved Vioxx. Merck had to aggressively promote the drug to be competitive with Celebrex.
    c. Merck could not allow negative study results to impact sales.
    d. Pharmaceutical companies often depend on developing blockbuster drugs. The success of Vioxx was considered crucial for the financial future of the company.
3. Comparative studies suggested that Vioxx had a higher number of CV events than Naproxen. Merck assumed that difference came not from Vioxx having any negative side effects but rather because Naproxen protected patient's hearts.
4. Drug companies have no incentives to do Phase IV (post approval) studies or to publish negative results from internal studies.
5. Most clinical research on drugs is sponsored by companies that make them. Drug companies now have more control than in past on the way the research is carried out and reported.
6. Merck had a reputation to maintain. Withdrawing Vioxx from the market and acknowledging CV events would have hurt their reputation.
7. The drug pipeline was dwindling and older drugs were going off patent protection. Merck was about to lose five of its most profitable patents.
8. Drug companies have no incentive to do Phase IV safety testing, even if it is required by the FDA. Similarly, they have no incentives to publish negative internal studies.

기사의 마케팅 모음집이었다.

멘탈 모델

1. 머크社는 원래 바이옥스가 심혈관 이벤트를 일으키지 않는다고 믿었다.
2. 머크社는 부정적인 결과 발표를 실제로 제한하고 잠재적인 심혈관 리스크에도 불구하고 의사들이 약을 처방하도록 설득한다면, 바이옥스가 블록버스터급 의약품이 될 수 있고 상당한 수익원이 될 수 있다고 생각했다.
3. 회사는 부정적인 결과를 숨김으로써 회사의 명성을 보호할 수 있을 것이라고 생각했다.
4. 잠재적 심혈관 리스크에도 불구하고 의사들이 약물을 처방하도록 설득할 수 있다고 믿었다.

컨텍스트:

1. 머크社는 주주들에게 투자 수익을 제공할 의무가 있고 주주들은 높은 수익을 요구한다. 게다가, 제약회사 임원들은 일부 보수를 스톡옵션으로 받는다.
2. 재정 결과의 만족도는 바이옥스가 블록버스터가 되는 것에 달려 있었다.
   a. 바이옥스는 머크社의 주 수입원이었고 수익성이 매우 높았다.
   b. 바이옥스는 FDA의 승인을 받기 5개월 전에 FDA의 승인을 받은 셀레브렉스(Celebrex)와 치열한 경쟁에 직면했다. 머크社는 셀레브렉스와 경쟁하기 위해 공격적으로 의약품을 홍보해야 했다.
   c. 머크社는 부정적인 연구 결과가 매출에 영향을 미치는 것을 허용할 수 없었다.
   d. 제약회사들은 보통 블록버스터급 의약품을 개발하는 데 의존한다. 바이옥스의 성공은 회사의 향후 재정에 매우 중요하다고 여겨졌다.
3. 비교 연구에서는 바이옥스의 심혈관 이벤트가 나프록센(Naproxen)보다 더 많았다고 명시되어 있었다. 머크社는 둘의 차이점이 바이옥스가 부정적인 부작용을 가지고 있는 것 때문이 아니라 나프록센이 환자의 심장을 보호했기 때문이라고 추정했다.
4. 제약회사들은 4단계(사후 승인) 연구를 하거나 내부 연구의 부정적인 결과를 발표할 동기가 없다.
5. 약물에 대한 대부분의 임상 연구는 해당 약물을 만드는 회사의 후원을 받는다. 현재 제약회사들은 연구가 수행되고 보고되는 방식에 대해 과거보다 더 많은 통제권을 가지고 있다.
6. 머크社는 유지해야 할 명성이 있었다. 바이옥스를 시장에서 회수하고 심혈관 이벤트를 인정하는 것은 그들의 명성을 손상시킬 것이다.
7. 약물 파이프라인이 점점 줄어들고 있었고 오래된 약물들이 특허권 보호에서 벗어나고 있었다. 머크社는 수익성이 가장 높은 특허 중 5개를 곧 잃게 될 수도 있었다.
8. 제약회사들은 FDA가 요구하더라도 4단계 안전성 검사를 할 동기가 없다. 마찬가지로, 그들은 부정적인 내부 연구를 발표할 동기가 없다.

## FDA/CDER

*Background Information*

The section within the FDA responsible for human drugs is called the Center for Drug Evaluation and Research (CDER). Within CDER, the Office of New Drugs (OND) is in charge of approving new drugs, setting drug labels and, when required, recalling drugs. The Office of Surveillance and Epidemiology (OSE) focuses on identifying adverse events that were not detected during the approval of drugs and can recommend actions, such as label changes or recalls, to OND.

Responsibilities:

*Committee Staff*

1. Select competent advisory committee members and establish and enforce conflict of interest rules.
2. Provide researchers access to accurate and useful adverse events reports.

*Office of New Drugs (OND)*

1. Oversee all U.S. human trials and development programs for investigational medical products to ensure safety of participants in clinical trials. Provide oversight of IRBs (Institutional Review Boards) that perform these functions for the FDA.
2. Set the requirements and process for the approval of new drugs.
3. Critically examine a sponsor's claim that a drug is safe for intended use. Impartially evaluate new drugs for safety and efficacy and approve them for sale if deemed appropriate.
4. Upon approval set the label for the drug.
5. Do not unnecessarily delay drugs that may have a beneficial effect.
6. Require phase IV safety testing if there is a potential long-term safety risk.
7. Remove a drug from the market if new evidence shows that the risks outweigh the benefits.
8. Update the label information when new information about drug safety is discovered.

*Division of Drug Marketing, Advertising, and Communications (DDMAC)*

1. Monitor the marketing and promotion of drugs. Review advertisements for accuracy and balance.

*Office of Surveillance and Epidemiology (OSE)*

1. Conduct on-going reviews of product safety, efficacy, and quality. Perform statistical analysis on adverse event data received to determine whether there is a safety problem.
2. Re-assess risks based on new data learned after a drug is marketed and recommend ways to manage risk.
3. Serve as consultants to OND with regards to drug safety issues.
4. Recommend that a drug be removed from the market if new evidence shows significant risks.

## FDA/CDER

***배경 정보***

FDA 내의 사람에 대한 약물(human drug) 부문은 약물 평가 연구 센터(CDER, Center for Drug Evaluation and Research)라 불리는 곳에서 담당한다. CDER 내에서 신약사무국(OND, Office of New Drugs)은 신약 승인, 의약품의 라벨 설정을 담당하며 필요한 경우 의약품의 리콜을 담당한다. 감시역학사무국(OSE, Office of Surveillance and Epidemiology)은 의약품 승인 중에 검출되지 않은 부작용 식별에 초점을 맞추고 있으며 라벨 변경이나 리콜과 같은 조치를 신약사무국에 권고할 수 있다.

책임:

*위원회 위원*

1. 유능한 자문위원을 선정하여 이해 상충 규칙을 수립하고 시행한다.
2. 연구자들이 정확하고 유용한 부작용 보고서에 접근할 수 있도록 한다.

*신약사무국(OND)*

1. 임상 시험 참가자의 안전을 보장하기 위해 시험용 의약품에 대한 미국의 모든 임상 시험과 개발 프로그램을 감독한다. FDA를 위해 이러한 기능을 수행하는 IRB(Institutional Review Board)를 감독한다.
2. 신약 승인을 위한 요건과 절차를 설정한다.
3. 약물의 사용이 안전하다는 스폰서의 주장을 비판적으로 검토한다. 신약의 안전성 및 효능을 공정하게 평가하고 적절하다고 판단될 경우 판매를 승인한다.
4. 승인되면 약물의 라벨을 설정한다.
5. 유익한 효능이 있을 수 있는 약물을 불필요하게 지연시키지 않는다.
6. 잠재적인 장기적 안전 리스크가 있는 경우 4단계 안전 시험을 요구한다.
7. 리스크가 이익보다 크다는 새로운 증거가 나타나면 시장에서 약물을 회수한다.
8. 약물의 안전에 대한 새로운 정보가 발견되면 라벨 정보를 업데이트한다.

*약물 마케팅, 광고 및 커뮤니케이션 부서(DDMAC)*

1. 약물의 마케팅과 홍보를 모니터링한다. 정확성과 밸런스를 위해 광고를 검토한다.

*감시역학사무국(OSE)*

1. 제품의 안전성, 효능, 품질에 대해 지속적인 검토를 실시한다. 안전 문제 여부를 결정하기 위해 접수된 부작용 데이터에 대해 통계 분석을 수행한다.
2. 약물 판매 후 습득한 새로운 데이터를 기반으로 리스크를 재평가하고 리스크 관리 방안을 권고한다.
3. 약물 안전 문제와 관련하여 신약사무국의 컨설턴트로써의 역할을 수행한다.
4. 새로운 증거가 중대한 리스크를 보인다면 시장에서 약물을 회수하도록 권고한다.

Role Played:

Agency Wide

1. Allowed waivers of conflict of interest rules for advisory panel members.
2. Pressured an FDA employee to change conclusions and recommendations on a study of Vioxx and prevented publication of the results.
3. Was not able to provide quality adverse event reports for researchers to use.

OND

1. Gave expedited review and approval to Vioxx even though the drug did not meet the criteria for expedited review.
2. Did not check whether clinical trial safety requirements were being enforced (e.g., that protocol 078 had an active DSMB).
3. Approved Vioxx without requiring a Phase IV study even though the long term risks were unclear.
4. Did not update the Vioxx label in a timely fashion.
5. Delayed the recall of Vioxx. Did not act fast or effectively enough.

DDMAC

1. Original warning letter was not followed by subsequent warnings; false and misleading promotional material went un-reviewed.

OSE

1. Did not properly monitor the drug for long-term risks. Could not differentiate normal adverse events from the ones due to the drug within the population affected.
2. Did not insist that Merck launch a large-scale clinical trial when suspicions first arose.
3. Did not require a recall of the drug.

수행한 역할:

Agency Wide

1. 자문 위원들 간의 상충되는 이해 규칙에 대한 면제를 허용했다.
2. FDA 직원에게 바이옥스 연구에 대한 결론과 권장사항을 변경하도록 압력을 가했으며 결과 공개를 막았다.
3. 연구자들이 사용할 수 있는 양질의 부작용 보고서를 제공하지 못했다.

OND(신약사무국)

1. 바이옥스가 우선 검토 기준을 충족하지 못했음에도 불구하고 우선 검토 및 승인을 하였다.
2. 임상시험의 안전 요구사항이 시행되고 있는지를 확인하지 않았다(예: 프로토콜 078에 활동 중인 DSMB(데이터 및 안전 모니터링 위원회)가 있음).
3. 장기적인 리스크가 불명확한데도 4단계 연구를 요구하지 않고 바이옥스를 승인했다.
4. 바이옥스 라벨을 적시에 업데이트하지 않았다.
5. 바이옥스의 회수를 지연시켰다. 신속하고 효과적으로 행동하지 않았다.

DDMAC(약물 마케팅, 광고 및 커뮤니케이션 부서)

1. 기존 경고문에 대한 후속 경고가 뒤따르지 않았다; 허위 및 오해의 소지가 있는 홍보 자료가 재검토되지 않았다.

OSE(감시역학사무국)

1. 약물에 대한 장기적인 리스크를 적절하게 모니터링하지 않았다. 영향을 받는 모집단 내에서 약물로 인한 부작용과 일반적인 부작용 사례를 구분할 수 없었다.
2. 처음에 의혹이 생겼음에도 불구하고 대규모 임상시험을 하는 것에 대해 문제를 제기하지 않았다.
3. 약물의 리콜을 요구하지 않았다.

Context in Which Decisions Were Made:

Agency Wide

1. Lack of strong leadership at the head of the FDA, high turnover and unfilled positions.
2. Tensions between the Office of New Drugs (OND) and the Office of Surveillance and Epidemiology (OSE). OND was much larger than OSE and had more resources. When OSE proposes to recall a drug, it is perceived as a failure of OND.
3. PDUFA: The FDA is partly sponsored by the pharmaceutical companies it is supposed to monitor and regulate. This leads to (a) pressure to reduce approval time and (b) comparatively less staff in safety monitoring and marketing oversight than in approval.
4. Limited resources in personnel and budget.
5. Many of the experts who are asked to be on an advisory panel work with the pharmaceutical companies. It is difficult to find experts who do not have such ties.
6. Political and congressional pressures (e.g., anti-regulatory climate, special interests).

OND

1. For pre-market review, the FDA only has information provided by the company with no other independent research data.
2. Legislation inhibits full disclosure of information: Clinical information is kept secret and the FDA cannot share proprietary data for independent analysis.
3. The FDA is unable to keep track of ongoing clinical trials.
4. Legislation makes it difficult for the FDA to require label changes.
5. A very high certainty that the drug is dangerous is required before the drug is recalled.
6. OND is in charge of both approving and recalling drugs.
7. PDUFA fees represent more than 50% of ODN's budget; The FDA depends on PDUFA funding which affects the decision-making process.

OSE

1. No independent decision-making responsibility.
2. High turnover of OSE directors.
3. No control over selective publication (companies are not required to publish results from clinical trials or even the fact that clinical trials were being conducted).
4. No legal authority to require additional safety studies once a drug is approved. Post-marketing safety requirements are rarely enforced.
5. Adverse event reporting is limited: reporting voluntary, no certainty the event was actually due to the product, reports often not detailed enough for use. Researchers do not know how many people are taking the medication so cannot use the Adverse Event Reporting System' (AERS) data to calculate incidence in the population.
6. Very limited sources of information about adverse events.

The rest of the analysis is omitted here but a link to the thesis on this topic is in Appendix A.

결정이 이루어진 컨텍스트:

Agency Wide

1. FDA 수장의 강력한 리더십 부재, 높은 이직률과 채용 공백
2. 신약사무국(OND)과 감시역학사무국(OSE) 사이의 긴장관계. OND는 OSE보다 규모가 훨씬 컸으며, 더 많은 자원을 가지고 있었다. OSE가 약물의 리콜을 제안하면 이것은 OND의 실패로 인식된다.
3. PDUFA: FDA는 모니터링 및 규제의 대상이 되는 제약회사들로부터 일부 후원을 받는다. 이는 (a) 승인 시간을 단축해야 한다는 압박과 (b) 승인 담당 직원보다 안전 감시 및 마케팅 감독 담당 직원이 상대적으로 적은 상황을 초래한다.
4. 인력과 예산 자원이 제한되었다.
5. 자문위원단의 많은 전문가들이 제약회사와 협력하고 있다. 이런 유대 관계가 없는 전문가를 찾는 것은 어렵다.
6. 정치적 압박과 의회의 압박(예: 규제 방지 분위기, 특수한 이해관계)

OND(신약사무국)

1. FDA는 시판 전 검토를 위해 다른 독립적인 연구 데이터 없이 회사가 제공하는 정보만 가지고 있다.
2. 정보의 완전 공개를 금지하는 법률: 임상 정보는 비밀로 유지되며 FDA가 독자적인 분석 데이터를 공유할 수 없다.
3. FDA가 진행 중인 임상시험을 파악할 수 없다.
4. 법 제정으로 인해 FDA가 라벨 변경을 요구하기 어렵다.
5. 의약품을 회수하기 전에 해당 의약품의 위험에 대한 높은 확실성이 필요하다.
6. OND는 의약품의 승인과 리콜을 모두 담당한다.
7. PDUFA 수수료는 ODN 예산의 50% 이상을 차지한다; FDA는 의사결정 과정에 영향을 미치는 PDUFA 기금에 의존한다.

OSE(감시역학사무국)

1. 독립적인 의사결정 책임이 없다.
2. OSE 이사(directors)의 이직률이 높다.
3. 선택적 출판에 대한 통제력이 없다(회사는 임상시험 결과를 게시하거나 임상시험이 수행되고 있다는 사실을 공개할 필요가 없다).
4. 약물이 승인되면 추가적인 안전 연구를 요구할 법적 권한이 없다. 시판 후 안전 요구사항은 거의 강제되지 않는다.
5. 부작용의 보고가 제한된다: 자발적인 보고가 부족하고, 부작용이 실제로 제품으로 인한 것인지 확실하지 않으며, 보고서가 사용하기에 충분히 상세하지 않다. 연구자들은 얼마나 많은 사람들이 그 약을 복용하고 있는지 모르기 때문에 모집단에서의 발병률(incidence)을 계산하기 위한 AERS(Adverse Event Reporting System) 데이터를 사용할 수 없다.
6. 부작용에 대한 정보의 출처가 매우 제한적이다.

나머지 분석은 여기서 생략하지만 이 주제에 대한 논문 링크는 부록 A에 있다.

## 2008 Financial Crisis Example

Melissa Spencer, in a 2012 MIT Master's thesis, demonstrated how CAST could be used to understand the collapse and rapid acquisition of the investment bank Bear Stearns in March 2008. Only a small part of the CAST analysis is included here. See Appendix A for a link to the complete thesis.

Loss Event: Bank Insolvency

Definition: Solvency is defined as satisfying the basic equation Assets = Liabilities + Equity. Insolvency occurs when this equation does not hold.

Hazards:

H1: Bank cannot pay debts (illiquid assets)
- Safety Constraint: Bank must be able to pay debts as they come due
- Safety Constraint: Bank must have adequate short-term assets and/or capital to cover short-term liabilities.

H2: Bank has greater liabilities than assets less equity
- Safety Constraint: Bank must always have a solvent balance sheet
- Safety Constraint: Bank must not acquire liabilities that exceed its assets and capital

H3: Market is unable to determine value of a financial instrument
- Safety Constraint: Market Participants must be able to determine value of market instruments
- Safety Constraint: All financial instruments traded in the market must have adequate information available to determine their inherent relative value.

H4: Market is unable to determine creditworthiness of institution
- Safety Constraint: Market Participants must be able to determine creditworthiness of bank
- Safety Constraint: There must be a clear and unbiased source of information about Bank's health available to the market

The primary components involved in the loss were:

- Asset Contributors
  - Traders at firm (buy and sell assets on the market)
  - Creditors to the firm (lend money or assets to firm)
  - Clients of the firm (provide fees and assets)
- Liability Controllers:
  - Management of Bear Stearns (responsible for protecting shareholders and managing risk
  - Traders at Bear Stearns (responsible for day to day balance sheet)
- Equity Contributors: Shareholders
- Federal Reserve Bank:
  - Overseas markets, sets interest rates, serves as lender of last resort to commercial banks
- Securities and Exchange Commission
  - Monitors balance sheets and health of investment banks
  - Monitors details of securities on the market
- U.S. Department of Treasury

## 2008년 금융 위기 사례

멜리사 스펜서(Melissa Spencer)는 2012년 MIT 석사 논문에서 2008년 3월 투자은행 베어 스턴스(Bear Stearns)의 붕괴와 신속한 인수에 CAST가 활용될 수 있는 방법을 제시했다. CAST 분석의 일부분만 여기에 포함된다. 전체 논문에 대한 링크는 부록 A를 참조한다.

손실 이벤트: 은행 파산

정의: 지급능력은 다음의 기본 방정식을 충족하는 것으로 정의한다.

자산(Assets) = 부채(Liabilities) + 자본(Equity)

이 방정식이 성립되지 않을 때 지급불능이 발생한다.

위험:

H1: 은행이 빚을 갚을 수 없다(부동자산)

안전 제약사항: 은행은 만기일에 빚을 갚을 수 있어야 한다.

안전 제약사항: 은행은 단기 부채를 충당하기 위해 적당한 단기 자산 및/또는 자본을 보유해야 한다.

H2: 은행이 자산에서 자본을 뺀 금액보다 부채가 더 많다.

안전 제약사항: 은행은 대차대조표 상 항상 지급 능력이 있는 상태(solvent)를 유지해야 한다.

안전 제약사항: 은행은 자산과 자본을 초과하는 부채를 취득해서는 안 된다.

H3: 시장이 금융상품의 가치를 결정할 수 없다.

안전 제약사항: 시장 참여자가 시장 상품의 가치를 결정할 수 있어야 한다.

안전 제약사항: 시장에서 거래되는 모든 금융상품에는 고유한 상대적 가치를 결정할 수 있는 충분한 정보가 있어야 한다.

H4: 시장이 기관의 신용도를 결정할 수 없다.

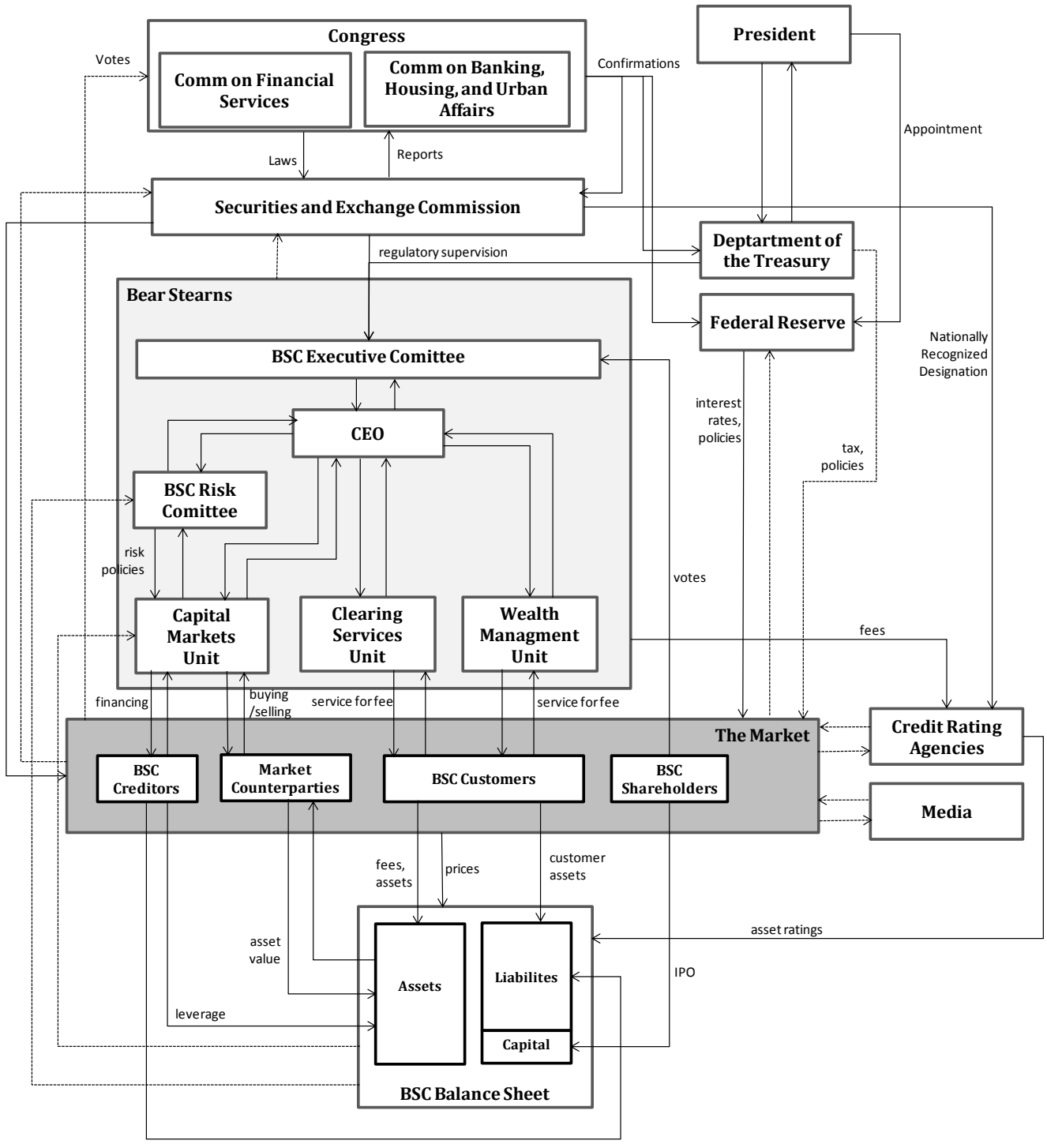
안전 제약사항: 시장 참여자가 은행의 신용도를 결정할 수 있어야 한다.

안전 제약사항: 은행의 건전성에 대한 명확하고 편견이 없는 정보가 시장에 제공되어야 한다.

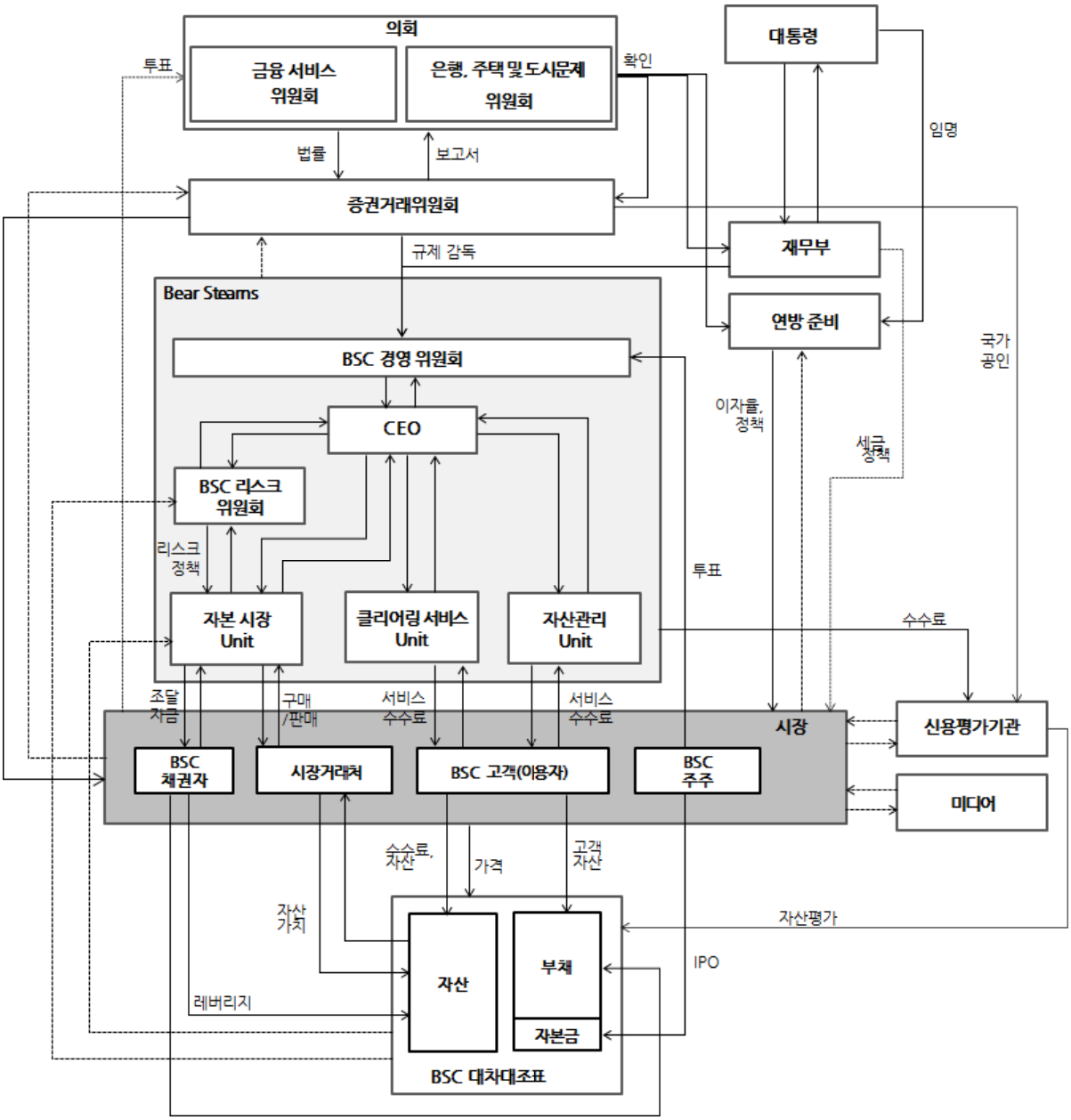
손실에 관련된 주요 구성요소는 다음과 같다.

- 자산 제공자(Asset Contributors)
  - 기업 트레이더(시장에서 자산을 매입·매도함)
  - 기업 채권자(기업에게 돈이나 자산을 빌려줌)
  - 기업 고객(수수료 및 자산 제공)
- 부채 관리자(Liability Controllers):
  - 베어 스턴스 경영진(주주 보호 및 리스크 관리 책임)
  - 베어 스턴스 증권 매매업자(매일의 대차대조표 담당)
- 자본 제공자(Equity Contributors): 주주
- 연방 준비 은행(Federal Reserve Bank):
  - 해외시장, 금리 책정, 시중은행의 최후의 대출 기관으로서 역할
- 증권거래위원회(Securities and Exchange Commission)
  - 투자은행의 대차대조표 및 건전성 모니터링
  - 증권시장의 유가 증권 세부사항 모니터링
- 미국 재무부(U.S. Department of Treasury)

Control Structure:



컨트롤 스트럭처:


의회
금융 서비스 위원회
은행, 주택 및 도시문제 위원회
투표
확인
법률
보고서
대통령
임명
증권거래위원회
재무부
규제 감독
Bear Stearns
BSC 경영 위원회
연방 준비
국가 공인
CEO
이자율, 정책
세금 정책
BSC 리스크 위원회
리스크 정책
투표
자본 시장 Unit
클리어링 서비스 Unit
자산관리 Unit
수수료
조달 자금
구매 /판매
서비스 수수료
서비스 수수료
시장
신용평가기관
BSC 채권자
시장거래처
BSC 고객(이용자)
BSC 주주
미디어
수수료, 자산
가격
고객 자산
자산 가치
자산평가
IPO
자산
부채
자본금
레버리지
BSC 대차대조표

Only one component of the CAST analysis is provided as an example here:

Federal Regulators of Investment Banks (Federal Reserve):

Responsibilities:

- Ensure banks are free of fraud or deceitful practices.
- Ensure banks are following basic practices to protect customers.
- Ensure adequate mechanisms for public knowledge of investments, investors have access to adequate knowledge of risks, conduct audits of bank practices, monitor markets.
- Ensure national economy is safe, monitor interconnectedness of financial system, ensure all institutions and instruments are properly regulated, protect federal resources.
- Detect and eliminate market externalities that arise in rapidly changing markets.

Contribution to losses:

- Allowed regulatory distinction between commercial and investment banks to erode without a corresponding change to regulatory protections for both institutional types.
- Did not distinguish between health of system and health of bankers/shareholders within system
- Allowed interconnectedness between regulated and unregulated entities to build.
- Did not ensure there was an unbiased (not paid for by banks) credit rating mechanism.
- Did not update regulatory requirements for investment bank balance sheet quickly enough
- Promoted housing policies that led to unsafe mortgages.
- Did not require disclosure from independent credit rating agencies on operations.

Process Model Flaws:

- Believed financial institutions would “self-regulate” in order to stay competitive.
- Believed failure of unregulated and lightly-regulated entities would only impact investors directly exposed to them.
- Believed mortgage-based securities were created safely, reflecting accurate risk profiles to investors.
- Believed failure of a single institution or instrument would not impact the entire financial system.

Context:

- Complicated regulatory scheme (Fed, SEC, FDIC, US Treasure, etc.) with different jurisdictions
- Political pressure for a “laissez-faire” economic policy
- Commercial banks seen as “safe" (given FDIC and Fed regulations) while investment banks were for more savvy investors with greater risk appetite
- Growing political and social power of banks, who generally support easing regulation
- Vast differences in compensation between regulators and those they regulate
- Rapidly changing market (new technologies, new instruments, new connections) was very difficult for regulators to keep up with
- Banks constantly looking for (and finding) regulatory loopholes
- Political pressure to encourage home ownership in 1990s and 2000s.

There are only a few attempts so far to use CAST for non-physical systems, but it appears that it can be done.

여기서는 CAST 분석의 일부만 예제로 제시한다:

투자 은행의 연방 규제 기관(연방 준비):

책임:

- 은행이 부정행위나 사기행위가 없는지 확인한다.
- 은행이 고객을 보호하기 위한 기본 관행을 준수하고 있는지 확인한다.
- 투자에 대한 일반인들의 지식을 위한 적절한 메커니즘을 보장하고 투자자는 리스크에 대한 적절한 지식에 접근하며, 은행의 관행에 대해 감사를 실시하고 시장을 모니터링한다.
- 국가 경제가 안전한지 확인하고 금융 시스템의 상호연결(interconnectedness)을 모니터링하며 모든 기관 및 기구가 제대로 규제되는지 확인하고 연방 자원을 보호한다.
- 급변하는 시장에서 발생하는 시장 외부성(externalities)을 탐지하고 제거한다.

손실에 대한 기여:

- 기관 유형(상업 은행, 투자 은행)에 따른 규제적 보호를 위한 변경을 수행하지 않음으로써 상업 은행과 투자 은행 간의 규제적 구분이 없어지도록 허용했다.
- 시스템 건전성과 시스템 내 은행원/주주의 건전성을 구분하지 않았다.
- 규제된 기업과 규제되지 않은 기업 간의 상호연결을 허용했다.
- 편향되지 않은(은행이 비용을 지불하지 않는) 신용 등급 체계가 있는지 확인하지 않았다.
- 투자 은행 대차대조표에 대한 규제 요구사항을 신속히 업데이트하지 않았다.
- 안전하지 않은 주택담보대출로 이어지는 주택 정책을 촉진했다.
- 독립적인 신용평가 기관에게 운영에 대한 공개를 요구하지 않았다.

프로세스 모델 결함:

- 금융 기관들이 경쟁력을 유지하기 위해 "자율 규제"를 할 것이라고 믿었다.
- 규제되지 않거나 규제가 미흡한 기업의 실패는 해당 기업에 직접적으로 관련된 투자자에게만 영향을 미칠 것이라고 믿었다.
- 주택담보대출 기반 증권은 투자자에 대한 정확한 리스크 프로파일을 반영하여 안전하게 만들어졌다고 믿었다.
- 단일 기관이나 기구의 실패가 전체 금융 시스템에 영향을 미치지는 않을 것이라고 믿었다.

컨텍스트:

- 관할 지역별 복잡한 규제 체계(Fed, SEC, FDIC, US Treasure 등)
- "자유방임주의(laissez-faire)" 경제 정책에 대한 정치적 압력
- 상업 은행은 (FDIC 및 Fed 규정에 따르면) "안전하다"고 간주되는 반면 투자 은행들은 보다 넓은 리스크 성향을 가진 명민한 투자자를 위한 것이다.
- 규제 완화를 전반적으로 지지하는 은행의 정치적, 사회적 힘이 성장하고 있다.
- 규제 기관과 그들이 규제하는 기관들 간의 보상 차이가 크다.
- 규제 기관은 급변하는 시장(새로운 기술, 새로운 상품, 새로운 연관성)을 따라잡기 매우 어려웠다.
- 은행들은 규제의 허점을 끊임없이 찾고 있다.
- 1990년대와 2000년대에 주택 소유를 장려하는 정치적 압력이 있었다.

비물리적(non-physical) 시스템에 CAST를 적용하려는 시도는 지금까지 몇 번밖에 없지만 수행할 수 있는 것으로 보인다.

# Chapter 6: Introducing CAST into an Organization or Industry

CAST involves a paradigm change in the way people think about and identify accident causes. Introducing it into an organization may require greater effort than simply changing notations or making small changes in the old paradigm. A few ideas to assist in making this change are presented here.

Paradigm changes of this sort often require enough dissatisfaction and frustration with the status quo by important participants in the organization or industry that natural lethargy can be overcome. A major accident involving large costs may assist in this process. But waiting for a major loss is clearly not the ideal way to introduce changes in how accident investigation is done. Demonstrations of how much more effective the new approach is when applied to previous accidents may be very helpful in both demonstrating practicality and benefits.

This approach is particularly effective when applied to losses in which CAST uncovers causes not found originally. Jon Hickey, a graduate student who was in the U.S. Navy, noticed that the Coast Guard experienced an increased aviation mishap rate where seven Class A mishaps occurred in the 22-month period between 2008 and 2010. The mishap investigations had centered on the pilots using HFACS, an accident causal analysis technique based on Reason's Swiss Cheese Model. The investigations did not find common contributing or causal factors. Commodore Hickey applied CAST, focusing on the systemic factors instead of human errors. Using CAST, he was able to identify the common factors leading to the losses. The HFACS analysis had stopped at identifying symptoms and did not identify the common systemic causes that were important in all the accidents.[24]

Introduction of new concepts will invariably lead to resistance in conservative, government organizations that are reluctant to introduce new ideas. Attempts to change established accident investigation processes have commercial, training, and contractual cost implications. The key in successfully introducing changes lies in being able to demonstrate that a new process is time efficient, is cost effective, and, most important, provides results that can significantly improve future safety. One potentially effective approach is to compare the results of accident reports published by well-regarded groups, such as the NTSB, based on a linear event model with a reanalysis of the same accident using a systems approach like CAST. We have been doing these types of comparisons, but more are still needed.

A powerful set of constituents can be created when the benefits of an explanatory vs. accusatory approach that does not focus on blame can be demonstrated. Groups, such as pilots who get the brunt of blame for accidents, are discovering the power of this new approach and providing support. Important player groups, such as unions, user-groups, and professional organizations that can exert pressure for change, may also be influential.

As with any paradigm change or cultural change, there must be buy-in at the top. Without high-level leadership, it is difficult to implement changes suggested at lower levels. Leadership willing to grab the opportunity to make changes after a major loss will be particularly effective. It is sad, but unfortunately too often true, that significant change is not possible without an event-driven disruption of complacency. More optimistically, significant changes and improvements can be driven by strong leaders. Paul O'Neill at Alcoa is an impressive example where he was able to both greatly reduce accidents while, at the same time, increase profits by focusing on safety as a primary goal. Basically, someone in authority has to decide that reducing losses is more important than continuing to do what they have always done.

[24] Jon Hickey, A System Theoretic Analysis of U.S. Coast Guard Aviation—CG-6505 Mishaps, STAMP Workshop, March 26, 2013, http://psas.scripts.mit.edu/home/

# 6장: 조직 또는 산업에 CAST 도입

CAST는 사람들이 사고의 원인을 생각하고 식별하는 방식에 대한 패러다임의 변경을 수반한다. 조직에 CAST를 도입하는 것은 단순히 표기법을 바꾸거나 기존 패러다임에 작은 변화를 주는 것보다 더 많은 노력이 필요할 수 있다. 이러한 변화를 돕기 위한 몇 가지 아이디어를 여기에 제시한다.

자연적인 무기력함을 극복할 수 있는 조직이나 산업에서, 이런 종류의 패러다임 변화는 핵심 구성원들이 현재 상황에 대해 많은 불만을 갖게 하고 좌절을 겪게 하는 경우가 많다. 많은 비용이 드는 중대 사고라면 변화 과정에서 도움이 될 수 있겠지만, 큰 손실이 발생하는 사고가 날 때까지 기다리는 것은 사고 조사 방법을 변화시키기 위한 좋은 방법은 분명히 아니다. 새로운 접근법을 이전의 사고에 적용하였을 때 얼마나 더 효과적인지를 보여주는 것은 실용성과 이점을 모두 입증하는 데 매우 유용할 것이다.

이러한 방법은 CAST를 적용하여 기존 조사에서 발견되지 않은 원인을 찾아내는 경우 특히 효과적이다. 미 해군에 재직했던 대학원생 존 히키(Jon Hickey)는 2008년부터 2010년까지 22개월 동안 7건의 A급 사고가 발생한 해안 경비대에서 항공 사고 발생률이 증가한 것을 발견했다. 리즌(Reason)의 스위스 치즈 모델을 기반으로 한 사고 원인 분석 기술인 HFACS를 통해 조종사를 중심으로 사고 조사가 이루어졌다. 사고 조사에서는 공통 요인이나 인과관계를 찾지 못했다. 히키 준장은 인적 오류 대신 시스템적 요소에 초점을 맞추어 CAST를 적용했다. 그는 CAST를 통해 손실로 이어지는 공통 요인을 식별할 수 있었다. HFACS 분석은 증상을 파악하는 단계에서 그쳤으며 모든 사고에서 중요한 공통적인 시스템 원인을 식별하지 못했다.[24]

새로운 개념의 도입은 새로운 아이디어의 도입을 꺼리는 보수적인 정부 조직의 저항으로 이어질 것이다. 확립된 사고 조사 프로세스를 변경하려는 시도는 상업적 비용, 훈련 비용 및 계약 비용의 변화를 초래한다. 변경을 성공적으로 도입하기 위한 열쇠는 새로운 프로세스가 시간 효율적이고 비용 효율적임을 입증하는 것이며, 가장 중요한 것은 미래의 안전을 크게 개선할 수 있는 결과를 가져온다는 것을 입증하는 것이다. 잠재적으로 효과적인 접근방식 중 하나는 NTSB와 같이 잘 알려진 그룹이 발행한, 선형 이벤트 모델에 기반한 사고 보고서의 결과를 CAST와 같은 시스템 접근방식을 사용하여 재분석한 결과와 비교하는 것이다. 우리는 이러한 유형의 비교를 해왔지만 여전히 더 많은 것이 필요하다.

비난에 초점을 맞추지 않는 설명적 접근법의 이점을 입증할 수 있을 때 강력한 지지자 집합을 만들 수 있다. 사고에 책임을 지는 조종사와 같은 그룹들은 이 새로운 접근법의 유용성을 발견하고 이 접근법의 활용을 지원하고 있다. 이러한 변화를 위해 압력을 행사할 수 있는 노조, 사용자 그룹, 전문 조직과 같은 중요한 참가자 그룹도 영향을 미칠 수 있다.

패러다임이나 문화의 변경에 있어서는 상부의 승인이 있어야 한다. 상위 수준의 리더십이 없다면 하위 수준에서 제시된 변경을 실행하기가 어렵다. 중대한 손실을 겪은 후, 변경 기회를 잡으려는 리더십이 특히 효과적일 것이다. 하지만 안타깝게도 사고의 발생 후 큰 손실 없이 사전에 중대한 변화를 꾀한다는 것이 불가능함은 자명한 사실이다. 보다 낙관적으로 보면 강력한 리더는 중요한 변경 및 개선을 주도할 수 있다. 알코아(Alcoa)社의 폴 오닐(Paul O'Neill)은 사고를 크게 줄이는 동시에 안전에 초점을 맞춰 수익을 올릴 수 있었던 인상 깊은 사례이다. 기본적으로 권한이 있는 사람은 그들이 항상 해왔던 것을 계속하는 것보다 손실을 줄이는 것이 더 중요하다는 결정을 해야 한다.

---

[24] Jon Hickey, A System Theoretic Analysis of U.S. Coast Guard Aviation—CG-6505 Mishaps, STAMP Workshop, March 26, 2013, http://psas.scripts.mit.edu/home/

A significant demonstration by smaller players in the industry may also be effective. CAST is being adopted by some smaller accident investigation authorities. Success shown by these efforts may lead others to follow.

There are additional practical questions that need to be answered. One is the cost of training people to think in a different way and use a new approach. Not everyone finds system thinking natural or easy. For a large organization that does its own internal investigation of incidents and accidents, a special group that is experienced in using CAST will get the best results. The investigation team should be independent of the management of the group in which the events occurred and report to a higher level of management. Having a trained group in the safety organization may be the most practical approach.

업계에서 소규모 참가자들의 의미 있는 시위도 효과적일 수 있다. CAST는 일부 소규모 사고 조사 당국에 의해 채택되고 있다. 이러한 노력들을 통해 성공을 거두면 다른 사람들이 따라갈 수 있다.

답변이 필요한 현실적인 질문들이 더 있다. 그 중 하나는 사람들이 다른 방식으로 생각하고 새로운 접근법을 사용하도록 훈련시키는 비용에 대한 것이다. 모든 사람이 시스템적 사고를 자연스럽고 쉽게 하는 것은 아니다. 사건 및 사고에 대한 자체 내부 조사를 수행하는 대규모 조직의 경우 CAST 활용 경험이 있는 특수 그룹이 있다면 최고의 결과를 얻을 수 있을 것이다. 조사팀은 이벤트가 발생한 그룹의 경영진으로부터 독립적이어야 하며 상위 수준의 경영진에게 보고해야 한다. 안전 조직에 훈련받은 그룹을 두는 것이 가장 현실적인 접근법일 것이다.

# Appendix A: Links to Published Examples of CAST Analyses of Real Accidents

Most of the analyses included here are by the author or her graduate students, with a couple of exceptions. Many were produced some time ago and may not include some of the more recent advances in CAST development. They do, however, at least show how CAST can be used in a variety of industries. I have not included the hundreds of analyses that have been done by students in my MIT graduate classes as they were limited in time and information and were just learning the technique. I also have not included industrial examples undertaken by others because of the proprietary nature of such accident analyses and privacy concerns.

**CAST Analysis of the Shell Moerdijk Accident** by Nancy G. Leveson

**Increasing Learning from Accidents: A Systems Approach Illustrated by the UPS Flight 1354 CFIT Accident** by Shem Malmquist, Nancy Leveson, Gus Larard, Jim Perry, and Darren Straker, May 2019

**The Underestimated Value of Safety in Achieving Organization Goals: CAST Analysis of the Macondo Accident.** by Maria Fernanda Tafur Munoz, MIT Engineering and Management Master's Thesis, June 2017.

**Systems-Theoretic Accident Model and Processes (STAMP) Applied to a U.S. Coast Guard Buoy Tender Integrated Control System.** by Paul D. Stukus, MIT SDM Masters Thesis, June 2017

**Learning from Accidents that are a consequence of complex systems.** by John Thomas and Shem Malmquist, ISASI Conference

**A Systems Approach to Analyzing and Preventing Hospital Adverse Events** by Nancy Leveson, Aubrey Samost, Sidney Dekker, Stan Finkelstein, and Jai Raman. *Journal of Patient Safety* , in press, 2016

**A STAMP Analysis of the LEX Comair 5191 Accident** , by Paul S. Nelson, Master's Thesis, Lund University, Sweden, June 2008, supervised by Prof. Sidney Dekker.

**Safety-Guided Design Analysis in Multi-Purposed Japanese Unmanned Transfer Vehicle.** by Ryo Ujiie, System Design and Management Master's Thesis, September 2016.

**Systems Theoretic Process Analysis Applied to an Offshore Supply Vessel Dynamic Positioning System.** by Blake Ryan Abrecht, MIT M.S. in Engineering Systems Thesis, June 2016.

**Systems Theoretic Accident Analysis of an Offshore Supply Vessel Collision.** by John Michael Mackovjak, Master of Science in Technology and Policy, MIT, June 2016.

**STAMP applied to Fukushima Daiichi nuclear disasteer and the safety of nuclear power plants in Japan.** by Daisuke Uesako, MIT Master's Thesis, System Design and Management Program, June 2016.

**System Theoretic Safety Analysis of the Sewol-Ho Ferry Accident in South Korea** , by Yisug Kwon, MIT Master's Thesis, December 2015.

**A Systems Approach to Patient Safety: Preventing and Predicting Medical Accidents Using Systems Theory,** by Aubrey Samost, MIT Master's Thesis, June 2015

**Comparison of SOAM and STAMP for ATM Incident Investigation** by Richard Arnold, Master's Thesis, Lund University, Sweden, 2009, supervised by Prof. Sidney Dekker.

# 부록 A: 실제 사고에 대한 CAST 분석 발표 사례 링크

본 보고서에 포함된 연구 대부분은 일부를 제외하고는 저자(Nancy G. Leveson)나 대학원 연구원들이 수행한 것이다. 과거에 수행한 많은 분석들은 최근 업데이트 된 CAST 내용을 일부 포함하지 않았을 수 있다. 그러나 이 분석 내용들은 최소한 CAST가 다양한 산업분야에서 어떻게 사용될 수 있는지를 제시한다. MIT 대학원생들이 수행했던 수백 건의 분석을 모두 포함하지는 않았다. CAST 분석을 하는데 있어 시간과 정보가 제한되어 있었고 학생들이 아직 기법을 익히는 단계였기 때문이다. 또한 이외 다른 곳에서 수행한 산업 사례를 포함하지 않았다. 이 같은 사고 분석 내용의 경우 특허권이나 개인정보보호의 우려가 있기 때문이다.

CAST Analysis of the Shell Moerdijk Accident by Nancy G. Leveson

Increasing Learning from Accidents: A Systems Approach Illustrated by the UPS Flight 1354 CFIT Accident by Shem Malmquist, Nancy Leveson, Gus Larard, Jim Perry, and Darren Straker, May 2019

The Underestimated Value of Safety in Achieving Organization Goals: CAST Analysis of the Macondo Accident. by Maria Fernanda Tafur Munoz, MIT Engineering and Management Master's Thesis, June 2017.

Systems-Theoretic Accident Model and Processes (STAMP) Applied to a U.S. Coast Guard Buoy Tender Integrated Control System. by Paul D. Stukus, MIT SDM Masters Thesis, June 2017

Learning from Accidents that are a consequence of complex systems. by John Thomas and Shem Malmquist, ISASI Conference

A Systems Approach to Analyzing and Preventing Hospital Adverse Events by Nancy Leveson, Aubrey Samost, Sidney Dekker, Stan Finkelstein, and Jai Raman. Journal of Patient Safety , in press, 2016

A STAMP Analysis of the LEX Comair 5191 Accident by Paul S. Nelson, Master's Thesis, Lund University, Sweden, June 2008, supervised by Prof. Sidney Dekker.

Safety-Guided Design Analysis in Multi-Purposed Japanese Unmanned Transfer Vehicle. by Ryo Ujiie, System Design and Management Master's Thesis, September 2016.

Systems Theoretic Process Analysis Applied to an Offshore Supply Vessel Dynamic Positioning System. by Blake Ryan Abrecht, MIT M.S. in Engineering Systems Thesis, June 2016.

Systems Theoretic Accident Analysis of an Offshore Supply Vessel Collision. by John Michael Mackovjak, Master of Science in Technology and Policy, MIT, June 2016.

STAMP applied to Fukushima Daiichi nuclear disasteer and the safety of nuclear power plants in Japan. by Daisuke Uesako, MIT Master's Thesis, System Design and Management Program, June 2016.

System Theoretic Safety Analysis of the Sewol-Ho Ferry Accident in South Korea, by Yisug Kwon, MIT Master's Thesis, December 2015.

A Systems Approach to Patient Safety: Preventing and Predicting Medical Accidents Using

**A CAST Analysis of a U.S. Coast Guard Aviation Mishap** , by Jon Hickey, MIT Master's Thesis, May 2012, supervised by Dr. Qi van Eikema Hommes.

**Application of CAST to Hospital Adverse Events** , by Meaghan O'Neil, MIT Master's Thesis, May 2014

**Application of CAST and STPA to Railroad Safety.** , by Airong Dong, MIT Master's Thesis, May 2012

**Engineering Financial Safety: A System-Theoretic Case Study from the Financial Crisis** , by Melissa Spencer, MIT TPP (Technology and Policy Program) Master's Thesis, May 2012

**A Systems Theoretic Application to Design for the Safety of Medical Diagnostic Devices** , by Vincent Balgos, MIT SDM Master's Thesis, February 2012, supervised by Dr. Qi van Eikema Hommes

**Application of a System Safety Framework in Hybrid Socio-Technical Environment of Eurasia.** by Azamat Abdymomunov, MIT SDM Thesis, 2011. This thesis won the "Best SDM Master's Thesis" award at MIT.

**A System Theoretic Safety Analysis of Friendly Fire Prevention in Ground Based Missile Systems,** by Scott McCarthy, MIT SDM Master's Thesis, January 2013

**Accident Analysis and Hazard Analysis for Human and Organizational Factors** by Margaret Stringfellow, October 2010

**A System Theoretic Analysis of the "7.23" Yong-Tai-Wen Railway Accident .** This paper, by Dajiang Suo from the Computer Science and Technology Dept., Tsinghua University, Beijing, China, was presented at the 1st STAMP/STPA Workshop held at MIT on April 26-28, 2012

**A Case Study of Vioxx using STAMP** by Matthieu Couturier, MIT Technology and Policy Master's Thesis, June 2010.

There are also several full examples in Nancy Leveson, *Engineering a Safer World*, MIT Press, 2012:

- Friendly Fire Shootdown of a U.S. Blackhawk Helicopter by a U.S. F-15 over the Iraqi No-Fly Zone, pp. 103-167
- The explosion of a Titan IV booster launched from Cape Canaveral in 1999, pp. 469-493
- The E. Coli Bacterial Contamination of a Public Water Supply in Walkerton, Canada, pp. 497-515

Finally, there is an academic paper I wrote about accident analysis that may interest some people:

**Applying Systems Thinking to Analyze and Learn from Events** by Nancy Leveson, *Safety Science*, Vol. 49, No. 1, January 2010, pp. 55-64

Systems Theory, by Aubrey Samost, MIT Master's Thesis, June 2015

Comparison of SOAM and STAMP for ATM Incident Investigation by Richard Arnold, Master's Thesis, Lund University, Sweden, 2009, supervised by Prof. Sidney Dekker.

A CAST Analysis of a U.S. Coast Guard Aviation Mishap, by Jon Hickey, MIT Master's Thesis, May 2012, supervised by Dr. Qi van Eikema Hommes.

Application of CAST to Hospital Adverse Events, by Meaghan O'Neil, MIT Master's Thesis, May 2014

Application of CAST and STPA to Railroad Safety, by Airong Dong, MIT Master's Thesis, May 2012

Engineering Financial Safety: A System-Theoretic Case Study from the Financial Crisis, by Melissa Spencer, MIT TPP (Technology and Policy Program) Master's Thesis, May 2012

A Systems Theoretic Application to Design for the Safety of Medical Diagnostic Devices, by Vincent Balgos, MIT SDM Master's Thesis, February 2012, supervised by Dr. Qi van Eikema Hommes

Application of a System Safety Framework in Hybrid Socio-Technical Environment of Eurasia. by Azamat Abdymomunov, MIT SDM Thesis, 2011. This thesis won the "Best SDM Master's Thesis" award at MIT.

A System Theoretic Safety Analysis of Friendly Fire Prevention in Ground Based Missile Systems, by Scott McCarthy, MIT SDM Master's Thesis, January 2013

Accident Analysis and Hazard Analysis for Human and Organizational Factors by Margaret Stringfellow, October 2010

A System Theoretic Analysis of the "7.23" Yong-Tai-Wen Railway Accident This paper, by Dajiang Suo from the Computer Science and Technology Dept., Tsinghua University, Beijing, China, was presented at the 1st STAMP/STPA Workshop held at MIT on April 26-28, 2012

A Case Study of Vioxx using STAMP by Matthieu Couturier, MIT Technology and Policy Master's Thesis, June 2010.

'Nancy Leveson, Engineering a Safer World, MIT Press, 2012'에도 몇 가지 사례가 포함되어 있다.

- 美 F-15가 이라크 비행 금지 구역 상공에서 미국 블랙호크 헬리콥터 아군 폭격으로 추락 (Friendly Fire Shootdown). pp.130-167
- 1999년 케이프 캐나베랄(Cape Canaveral)에서 발사된 타이탄 IV 부스터가 폭발. pp.469-493
- 캐나다 워커톤(Walkerton) 공공급수의 대장균 오염. pp.497-515

마지막으로, 사고 분석에 대해 필자가 작성한 연구 논문이 있다 :

Applying Systems Thinking to Analyze and Learn from Events by Nancy Leveson, Safety Science, Vol. 49, No. 1, January 2010, pp. 55-64

# Appendix B: Background Information and Summary CAST Analysis of the Shell Moerdijk Loss

**Background**:

On 3 June 2014, an explosion and fire occurred at the Shell Moerdijk plant in The Netherlands. Shell Moerdijk produces chemicals, such as ethylene and propylene, used to manufacture plastic products. Heat is first used to convert gasoil, naphtha, and LPG into a wide variety of chemicals. These chemicals are then used, among other things, as raw materials to produce other products at Shell Moerdijk, including those produced by the styrene monomer and propylene oxide (MSPO) plant involved in the accident.

Shell has two MSPO plants in Moerdijk: MSPO1 (commissioned in 1979) and MSPO2. The accident took place in the MSPO2 plant, which was designed in 1996 by the predecessor of what is now called Shell Projects and Technology,[25] the license-holder for the process. On the basis of a user agreement, Shell Moerdijk is responsible for the operation of the MSPO2 plant.

The MSPO plants produce styrene monomer and propylene oxide using ethylbenzene as the raw material. Styrene monomer is used for the production of polystyrene, a plastic that is used in a wide range of products such as polystyrene foam. Propylene oxide is used for the production of propylene glycol, which is used in food, cosmetics, medicines, and other products.

Worldwide, Shell has three more plants in which styrene monomer and propylene oxide are produced by means of a process that is virtually the same as at the MSPO2 plant. Two plants are located in Singapore, at a site called Seraya, and one plant is in Nanhai, China.

In general terms, styrene monomer and propylene oxide are produced as follows: Ethylbenzene reacts with oxygen whereby it is converted into ethylbenzene hydroperoxide. The ethylbenzene hydroperoxide then reacts with propylene with the help of a catalyst[26] and is converted into propylene oxide and methylphenylcarbinol and methylphenyl ketone. The methylphenyl ketone is a by-product of this reaction. In the last step, the methylphenylcarbinol is converted into styrene monomer. The by-product methylphenyl ketone is also converted into methylphenylcarbinol in a separate process step with the help of a different catalyst. It was in this final step of the process that the accident occurred.

The explosion was in the hydrogenation Unit (4800) of the MSPO2 plant. In the reactors of Unit 4800, hydrogen is used along with a catalyst to convert methylphenyl ketone into methylphenylcarbinol. This conversion, using hydrogen, is known as hydrogenation. The reaction with hydrogen in Unit 4800 releases heat, which is dissipated by allowing liquid ethylbenzene to flow along the catalyst in the reactors. The process is called “exothermic hydrogenation reaction.” It requires a pressure increase in the reactor. Because hydrogen is very flammable when combined with the increased pressure, fire can occur in the event of a leak. This hazard places important safety requirements on the design and operation of the Unit.

In general terms, Unit 4800 consists of two reactors, two separation vessels, a combined installation with which a liquid can be heated or cooled, and an installation for condensing the gas flow. The various parts of the Unit 4800 installation are interconnected by pipes and one central pump. See Figure B.1.

Liquids and gases from the reactor are separated from each other in the separation vessels. The gases from the first separation vessel go to reactor 2, and the gases from the second separation vessel

[25] Because I do not know the name of the predecessor organization, it will be referred to by the current name, Shell Projects and Technology, in this analysis.

[26] A catalyst is a substance that influences the rate of a specific chemical reaction.

# 부록 B: 쉘 뫼르딕(Shell Moerdijk) 손실의 배경 정보 및 CAST 분석 요약

**배경:**

2014년 6월 3일 네덜란드의 쉘 뫼르딕(Shell Moerdijk) 플랜트에서 폭발과 화재가 발생했다. 쉘 뫼르딕은 플라스틱 제품을 제조하는데 사용되는 에틸렌, 프로필렌과 같은 화학물질을 생산한다. 가스 오일, 나프타, LPG가 다른 여러 가지 화학물질로 변환되는데 열이 우선적으로 사용된다. 이렇게 변환된 화학물질은 쉘 뫼르딕에서 다른 제품을 생산하는 원료로 사용된다. 이는 사고와 관련된 스티렌 모노머(styrene monomer)와 프로필렌 옥사이드(propylene oxide) (MSPO) 플랜트에서 생산되는 제품의 원료로도 사용된다.

쉘은 뫼르딕에 MSPO1(1979년에 위임됨)과 MSPO2라는 두 개의 MSPO 플랜트를 가지고 있다. MSPO2 플랜트에서 사고가 일어났으며 1996년에 이 플랜트는, 플랜트 공정의 라이선스 소유자인 지금의 Shell Projects and Technology[25]라는 기관의 이전 기관(정확한 기관명은 모름)에 의해 설계되었다. 쉘 뫼르딕은 사용자 계약에 근거하여, MSPO2 플랜트의 운영을 책임지고 있다.

MSPO 플랜트는 에틸벤젠을 원료로 사용하여 스티렌 모노머와 프로필렌 옥사이드를 생산한다. 스티렌 모노머는 폴리스티렌, 즉, 플라스틱 생산에 사용되고 이 플라스틱은 폴리스티렌 폼과 같은 다양한 제품에 사용된다. 프로필렌 옥사이드는 식품, 화장품, 의약품 및 기타 제품에 사용되는 프로필렌 글리콜 생산에 사용된다.

쉘은 전 세계적으로 세 개의 플랜트를 더 보유하고 있다. 이 세 개의 플랜트에서는 MSPO2 플랜트와 거의 동일한 공정을 통해 스티렌 모노머 및 프로필렌 옥사이드를 생산한다. 2개의 플랜트는 싱가포르의 세라야(Seraya)에 있고, 나머지 플랜트는 중국 난하이(Nanhai)에 있다.

일반적으로 스티렌 모노머와 프로필렌 옥사이드는 다음과 같이 생산된다: 에틸벤젠은 산소와 반응하여 에틸벤젠 하이드로과산화물(hydroperoxide)로 전환된다. 그 후 에틸벤젠 하이드로과산화물은 촉매제[26] 작용을 통해 프로필렌과 반응하여 프로필렌 옥사이드와 메틸페닐카르비놀(methylphenylcarbinol)과 메틸페닐케톤(methylphenyl)으로 전환된다. 메틸페닐케톤은 이 반응의 결과로 생성된 부산물이다. 마지막 단계에서 메틸페닐카르비놀은 스티렌 모노머로 변환된다. 부산물인 메틸페닐케톤은 별도의 공정 단계에서 다른 촉매 작용을 통해 메틸페닐카르비놀로 전환된다. 이 마지막 단계에서 사고가 발생하였다.

MSPO2 플랜트의 수소화(hydrogenation) Unit 4800에서 폭발이 일어났다. Unit 4800의 반응로에서 수소는 촉매제와 함께, 메틸페닐케톤을 메틸페닐카르비놀로 전환하는 데 사용된다. 수소를 이용한 이러한 전환을 수소화라고 한다. Unit 4800에서 수소와 반응 시 열을 방출하는데, 이 열은 액체 에틸벤젠이 촉매제와 함께 반응로 내에서 흘러가면서 소멸된다. 이 과정을 "발열 수소화 반응"이라고 한다. 이것은 반응로의 압력을 증가시킨다. 수소가 증가된 압력과 결합하면 가연성이 매우 높기 때문에 누출되는 경우 화재가 발생할 수 있다. 이러한 위험은 Unit의 설계 및 운전에 중요한 안전 요구사항을 요구한다.

일반적으로 Unit 4800은 2개의 반응로, 2개의 분리 용기, 액체를 가열하거나 냉각시킬 수 있는 복합 설비 및 가스 흐름을 응축하는 설비로 구성된다. Unit 4800 설비의 다양한 부품은 여러 개의 파이프와 하나의 중앙 펌프에 의해 서로 연결된다. 이는 그림 B.1 참조하면 된다.

---

25 이전 조직의 명칭을 모르기 때문에 이 분석에서는 현재 이름인 쉘 프로젝트 앤 테크놀로지로 언급함.
26 특정 화학 반응의 비율에도 영향을 주는 촉매 역할을 해 주는 성분이다.

go to the flare (combustion). For, the separation vessel to function properly, it is important to achieve the correct ratio of gas and liquid. Various safety devices are used to achieve this goal.

The reactors contain a catalyst. The catalyst is used to accelerate the reaction between the substances being used in the reactors. In Unit 4800, the catalyst is in the form of cylindrical catalyst pellets. These are composed of different elements, including copper, chromium and barium. After a number of years of production, the effects of the catalyst decline and it has to be replaced. The catalyst pellets are replaced during a brief maintenance stop. The replacement of the pellets was uneventful in this case.

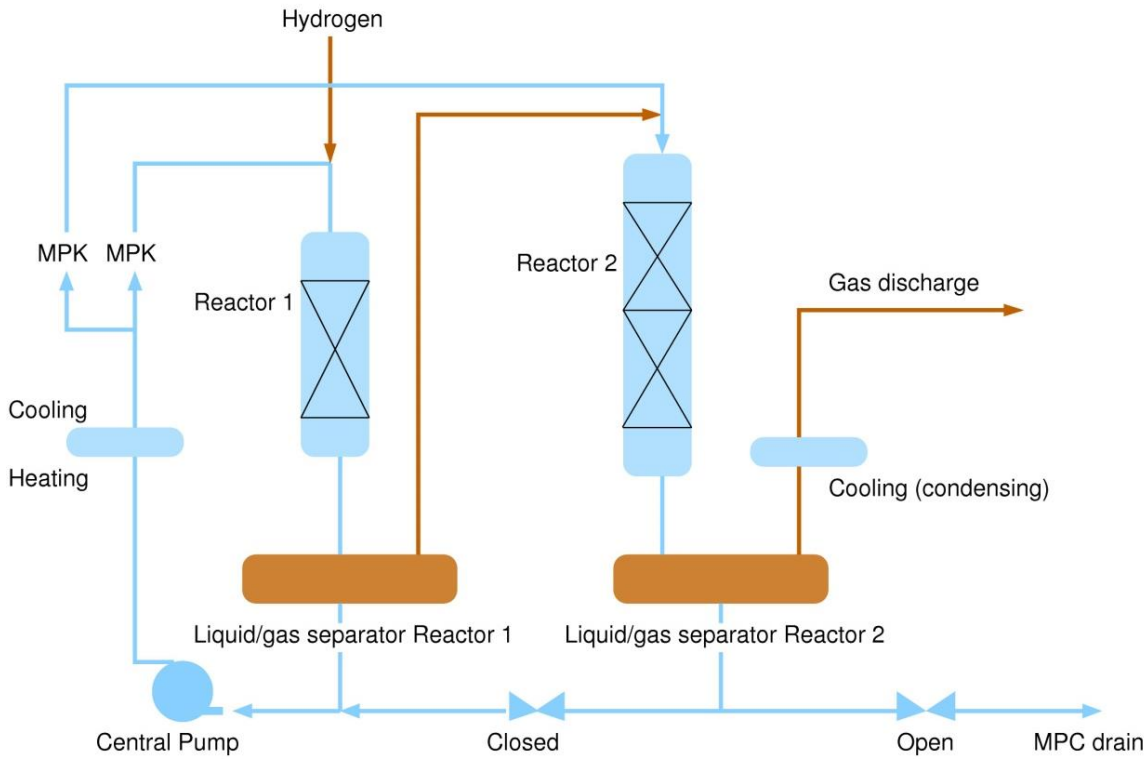



**Figure B.1:** Unit 4800 during normal production [taken from Dutch Safety Board report]

After the catalyst pellets have been replaced, Unit 4800 has to be restarted. This restart involves several steps: (1) release the oxygen from the Unit and then test for leaks; (2) flush the Unit with ethylbenzene to remove contamination; (3) fill the Unit with clean ethylbenzene and start circulating the ethylbenzene (called the *circulation phase*); (4) heat up the Unit (the *reheating phase*); and (5) reduce the catalyst using hydrogen (the *reduction phase*).

Circulating the ethylbenzene and heating the Unit (Steps 3 and 4) are necessary in order to wet the catalyst pellets and to raise the Unit temperature to a level that facilitates the reduction of the catalyst. The accident occurred during the reheating phase (Step 4).

반응로에서 나오는 액체와 기체는 분리 용기에서 서로 분리된다. 첫 번째 분리 용기의 가스는 반응로 2로 가고, 두 번째 분리 용기의 가스는 플레어(연소, combustion)로 간다. 분리 용기가 제대로 작동하기 위해서는 가스와 액체의 정확한 비율을 맞추는 것이 중요하다. 이러한 목적을 달성하기 위해 다양한 안전 장치가 사용된다.

반응로에는 촉매제가 들어있다. 이 촉매제는 반응로에 사용되는 물질 간의 반응을 가속화하는 데 사용된다. 촉매제는 Unit 4800에서 원통형(cylindrical) 촉매제 펠릿의 형태로 되어 있다. 이 촉매제 펠릿들은 구리, 크롬, 바륨 등의 다른 요소들로 구성되어 있다. 촉매제는 수년간의 생산과정에서 그 효과가 감소하기 때문에 반드시 교체되어야 한다. 촉매제 펠릿은 유지보수를 위한 짧은 가동정지 시기 중에 교체된다. 이 경우 펠릿의 교체는 전혀 문제가 되지 않았다.

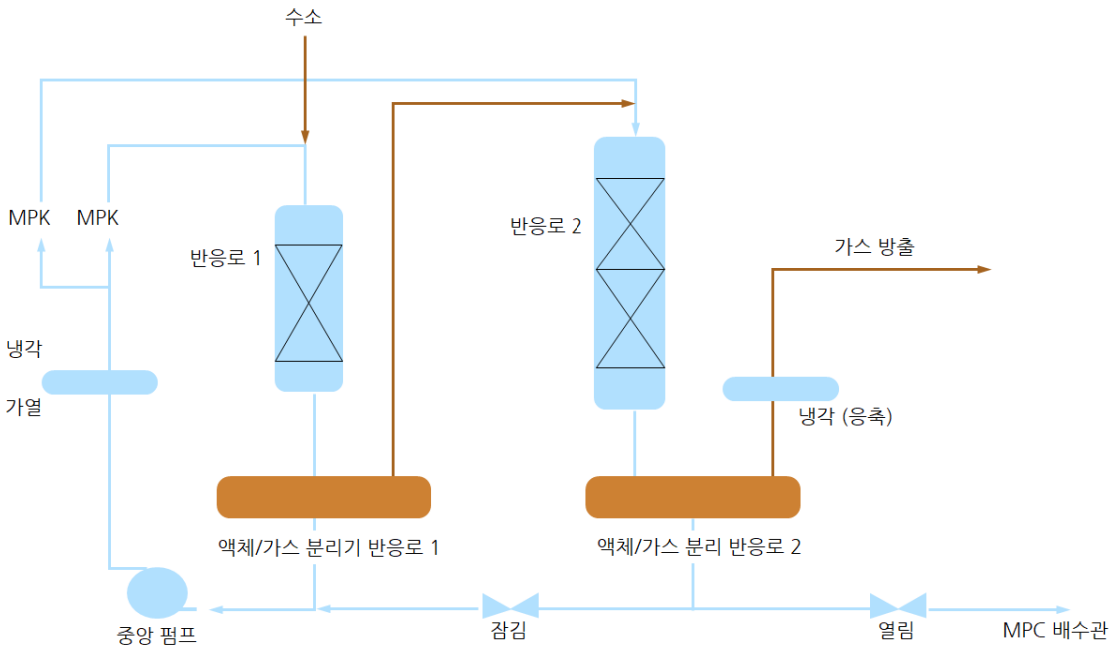



그림 B.1 : 정상 생산 과정의 Unit 4800 [네덜란드 안전위원회 보고서에서 발췌]

촉매제 펠릿을 교체한 후에는 Unit 4800을 재가동해야 한다. 이 재가동에는 다음과 같은 몇 가지 단계가 포함된다: (1) 유닛에서 산소를 방출한 후 누출을 테스트한다; (2) 오염을 제거하기 위해 유닛을 에틸벤젠으로 세척한다; (3) 유닛에 깨끗한 에틸벤젠을 채우고 에틸벤젠을 순환시키기 시작한다(*순환 단계*라고 함); (4) 유닛을 가열한다(*재가열 단계*); 그리고 (5) 수소를 이용하여 촉매제를 감소시킨다(*감소 단계*).

촉매제 펠릿을 적시고, Unit의 온도를 촉매제가 환원(reduction)되는 수준까지 상승시키기 위해서는 에틸벤젠 순환 및 Unit 가열 단계(단계 3 및 단계 4)가 필요하다. 재가열 단계(단계 4)에서 사고가 발생했다.

Thoroughly wetting the catalyst pellets in a trickle-bed reactor[27] is critical. Wetting involves fully soaking the catalyst with ethylbenzene and keeping the pellets continuously wet. If there are localized dry zones, the heat released from a reaction cannot dissipate. The result can be an undesirable rise in the temperature of the reactors. To ensure the catalyst pellets are wet down thoroughly, enough ethylbenzene and nitrogen must be allowed to flow through the reactors and the ethylbenzene must be well distributed. These requirements are achieved by feeding ethylbenzene (liquid) and nitrogen (gas) in the correct ratios through a distribution plate in the reactors, creating a "shower effect" that distributes the liquid optimally across the catalyst pellets.

Catalyst reduction (the fifth step in restarting the reactor) can begin once the plant is at the correct temperature and hot ethylbenzene has been circulated through it for at least 6 hours. Unit 4800 never reached this step on the evening of the accident due to explosions and fire during the heating phase.

Final Summary Causal Analysis and Recommendations Resulting from the CAST Analysis

In general, there were so many flaws in the Shell Safety Management System and the behavior of almost every component of Shell Global and Shell Moerdijk that a comprehensive redesign of the Shell and Shell Moerdijk safety management system and the safety information system would seem to be appropriate. In addition, there appear to be flaws in the safety culture that should be corrected. The oversight authorities also were ineffective in preventing the accident using their procedures and legislation and a review and redesign of the oversight procedures appears to be appropriate.

Figure B.2 shows the safety control structure assumed in the CAST analysis, with flawed control and feedback contributing to the accident shown with dotted lines. As can be seen, almost the entire structure was involved.

[27] Trickle-bed reactors (used in Unit 4800) have "open" columns filled with catalyst in which a gas and a liquid flow together in the same direction under the influence of gravity,

트리클베드(trickle-bed) 반응로[27]에서 촉매제 펠릿을 완전히 적시는 것은 매우 중요하다. 적신다고 하는 것은, 에틸벤젠으로 촉매제를 완전히 흠뻑 적시는 것과 펠릿을 젖은 상태로 계속 유지하는 것을 의미한다. 만약 부분적으로 마른 부분이 있으면 반응 시 방출되는 열이 소멸될 수 없다. 그 결과 반응로의 온도가 의도치 않게 상승할 수 있다. 촉매제 펠릿이 완전히 젖도록 하려면 충분한 에틸벤젠과 질소가 반응로를 통해 흐르도록 해야 하며 에틸벤젠이 잘 분포되도록 해야 한다. 이러한 요구사항은 에틸벤젠(액체)과 질소(가스)를 반응로 내의 분배 플레이트(distribution plate)를 통해 정확한 비율로 공급하여 촉매제 펠릿 전체에 액체를 최적으로 분배하는 "샤워 효과(shower effect)"를 만들어냄으로써 충족된다.

촉매제 감소(반응로 재가동의 5번째 단계)는 플랜트가 적정 온도에 있고 뜨거운 에틸벤젠이 최소 6시간 동안 그 온도에서 순환되어야 시작할 수 있다. 사고 당일 저녁, Unit 4800은 가열 단계 과정에서의 폭발과 화재로 인해 촉매제 감소 단계에 도달할 수 없었다.

CAST 분석의 최종 원인 분석 요약 및 권고사항

전반적으로 쉘 안전 관리 시스템과 쉘 글로벌 및 쉘 뫼르딕의 거의 모든 컴포넌트의 동작에 너무 많은 결함이 있었기 때문에 쉘 및 쉘 뫼르딕 안전 관리 시스템과 안전 정보 시스템의 종합적인 재설계가 필요해 보였다. 또한 안전 문화에도 개선되어야 할 문제점이 있는 것으로 밝혀졌다. 절차와 법률을 활용한 감독 당국의 사고 예방 또한 효과적이지 못했기 때문에 감독 절차에 대한 검토 및 재설계가 필요해 보였다.

그림 B.2는 CAST 분석에서 가정한 안전 컨트롤 스트럭처를 나타내며 사고에 기여한 결함 있는 컨트롤 및 피드백은 점선으로 나타내고 있다. 다음 그림과 같이 거의 모든 구조가 관련되어 있다.

27 (Unit 4800에서 사용되는) 트리플 베드(Trickle-bed) 반응로에는 기체와 액체가 중력의 영향으로 인해 동일한 방향으로 함께 흐르도록 되어 있는 촉매제로 채워진 "개방형" 기둥이 있다.

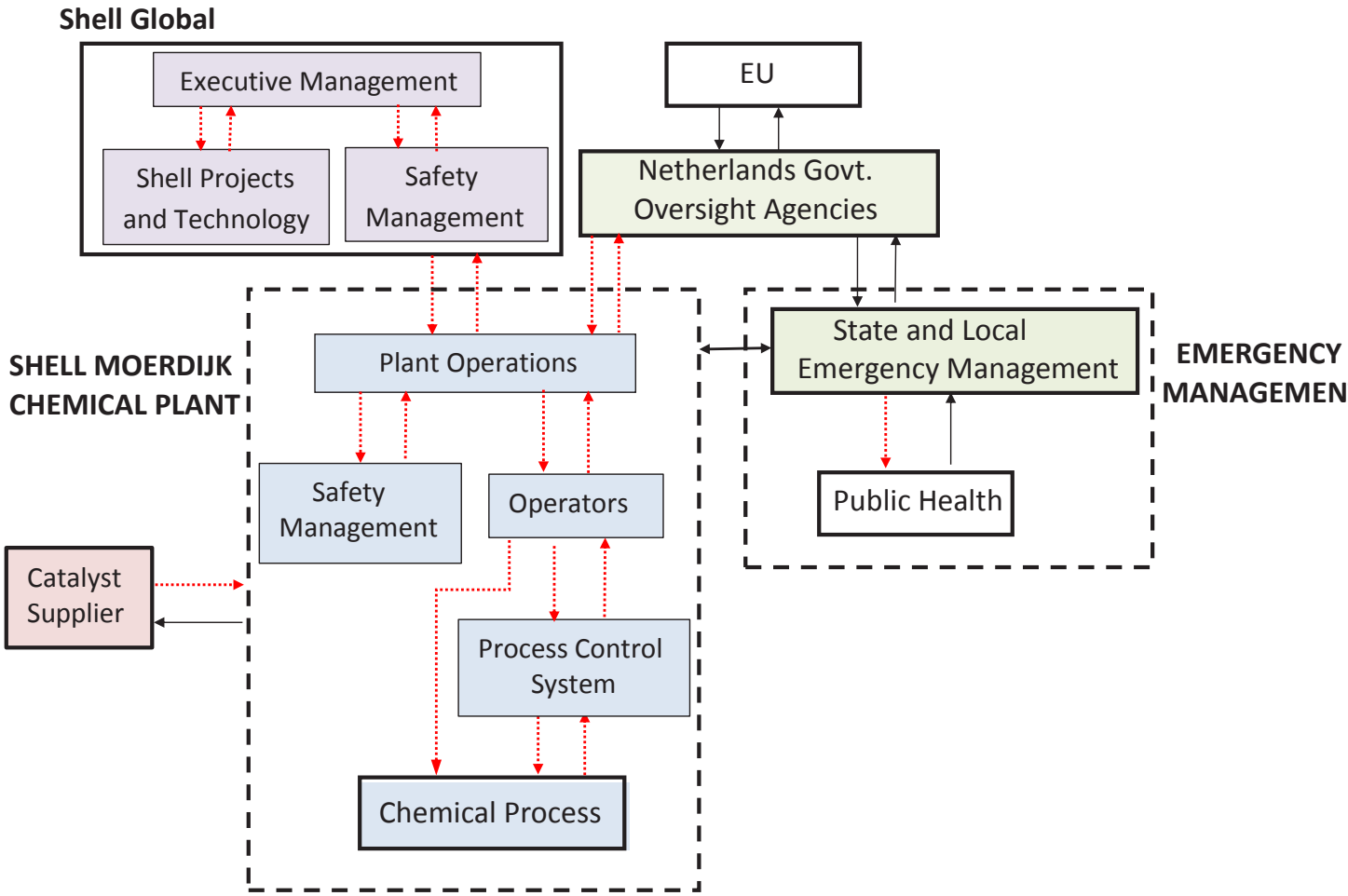



**Figure B.2:** Flawed Interactions in the assumed Safety Control Structure. Red dotted lines represent missing or inadequate control or feedback. Almost all the interactions were flawed in some way.

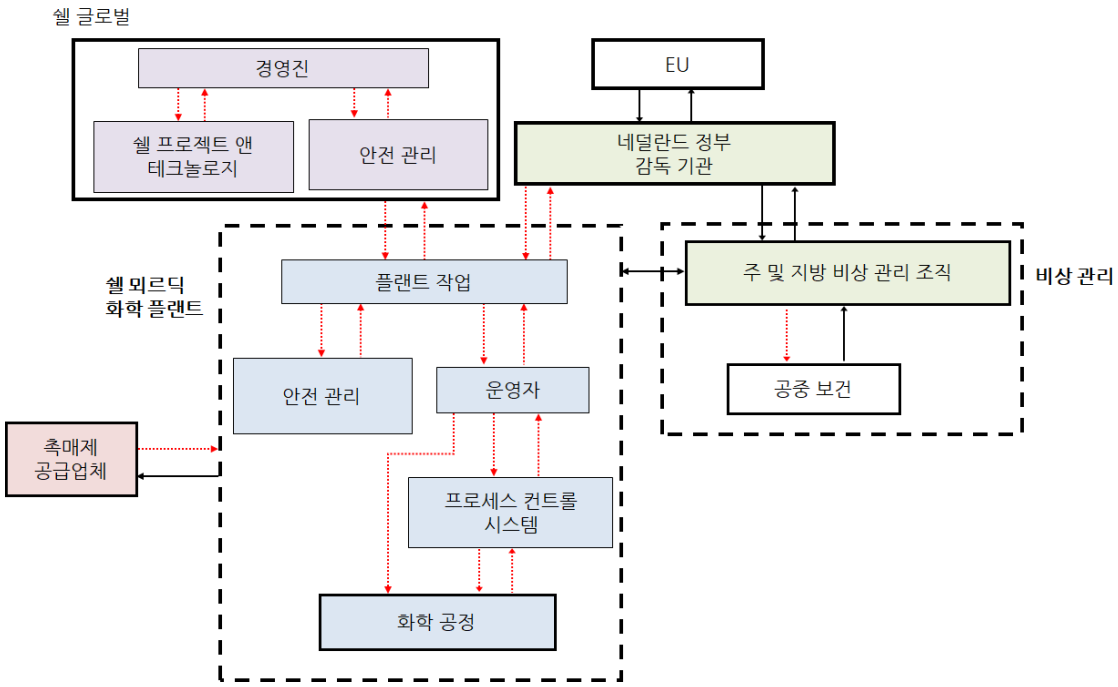



그림 B.2: 안전 컨트롤 스트럭처에서 결함이 있는 상호작용. 빨간색 점선은 컨트롤 또는 피드백이 누락되거나 부적절한 것을 나타냄. 어떤 면에서는 거의 모든 상호작용에서 어떤 식으로든 결함이 있었음.

As an overview of the CAST analysis results, the following table summarizes each component's role in the accident along with the recommendations generated for that component. The reasons for the component's role in the accident would probably be augmented if the unanswered questions noted in the CAST analysis details had been included in the accident report.

| | |
|---|---|
| Chemical Process | **Role:** None of the physical controls failed. The final physical collapse of the reactor and separation vessel after pressure reached a critical level resulted from unexpected and unhandled chemical and physical interactions. Many of these unsafe interactions were a result of design flaws in the reactor or in the safety-related controls.<br><br>**Recommendations**: The physical design limitations and inadequate physical controls need to be fixed. (The potential detailed fixes are not included here; they need to be determined by a qualified chemical engineer.) |
| Process Control System | **Role**: The process control system was not configured to provide the necessary help to the operators during a start-up or to allow them to easily stop the process in an emergency. The reason for these design decisions rests primarily in incorrect assumptions by the designers, who thought the accident scenario was impossible. Even after previous incidents at similar plants in which these assumptions were found to be untrue, the assumptions were not questioned and revisited.<br><br>**Recommendations**: The operators' knowledge and skill are most challenged during off-nominal phases, and most accidents occur during such phases and after changes are made or occur. The process control system should be redesigned to assist operators in all safety-critical, off-nominal operations (not just this restart scenario). For manual operations, the goal should be to provide all necessary assistance to the operators in decision making and in reducing attention and time pressures. |
| Operators | **Role**: The operators acted appropriately or at least understandably given the context, the incorrect work instructions (which they followed), and their lack of training needed to perform the work. In addition, they were provided with almost no assistance from the process control system, while many of the tasks they needed to do required intense attention, precision, mental effort, deep understanding of process dynamics, and frequent adjustments to a continually fluctuating process. The risks were not communicated properly.<br>Management relied on the operators seeing something strange and stopping the process, but did not provide the information and training the operators needed to do this.<br><br>**Recommendations**: The operators must have the appropriate skills and expertise to perform their assigned activities, and there must be someone assigned the responsibility for enforcing this requirement. A human factors study during the job analysis is needed to ensure that the operators are provided with the necessary information and work situation that allows them to make appropriate decisions under stressful conditions. Also, better automated assistance should be provided in all phases of operation, training should be provided for activities that are known to be hazardous like startup, and work instructions as well as the process for producing them need to be improved. |

다음 표는 CAST 분석 결과의 개요로서, 각 컴포넌트의 권고사항 및 사고에서의 역할과 함께 권고사항을 요약하여 제시하고 있다. 만일 사고 보고서의 CAST 분석 세부 내용 중에 답변이 없는 질문이 있었다면, 사고에서의 컴포넌트 역할의 이유는 더 많아졌을 것이다.

| | |
|---|---|
| 화학 공정 (Chemical Process) | **역할:** 어떠한 물리적 컨트롤도 실패하지 않음. 압력이 임계 수준에 도달한 후 예상치 못한 화학적 및 물리적 상호작용에 의해 반응로와 분리 용기의 최종적 붕괴가 일어났다. 이러한 안전하지 않은 상호작용의 대부분은 반응로나 안전 관련 컨트롤의 설계 결함 결과였다.<br><br>**권고사항:** 물리적 설계의 한계와 부적절한 물리적 컨트롤은 수정될 필요가 있다. (수정이 가능한 세부사항은 여기에 포함되지 않으며, 전문적인 화학 엔지니어가 확정하여야 한다.) |
| 프로세스 컨트롤 시스템 (Process Control System) | **역할:** 프로세스 컨트롤 시스템은 기동 과정에서 운영자에게 필요한 도움을 제공하거나 비상상황에서 프로세스를 쉽게 중단할 수 있도록 구성되어 있지 않았다. 이러한 설계 결정의 주된 이유는 설계자들이 사고 시나리오의 발생이 불가능하다고 잘못 가정한 것에 있다. 과거에 유사한 플랜트 사건에서 이러한 가정이 잘못된 것이라고 밝혀진 후에도 그 가정에 대한 의문이 제기되거나 재검토되지 않았다.<br><br>**권고사항:** 비정상적인(off-nominal) 상황에 대해 요구되는 운영자의 지식과 기술이 가장 어려운 문제이며, 대부분의 사고는 이러한 비정상적인 상황에서 발생하거나 변경이 일어난 후에 발생한다. 프로세스 컨트롤 시스템은 모든 안전 중요 작업 및 비정상적인 작업(단지 재구동 시나리오뿐만 아니라)을 하는 운영자를 지원하기 위해 재설계 되어야 한다. 수동 운전(manual operation) 과정에서의 목표는 의사결정을 하거나 주의력 및 시간 압박을 줄이는 데 필요한 모든 지원을 운영자에게 제공하는 것이 되어야 한다. |
| 운영자 (Operators) | **역할:** 운영자들은 주어진 상황, (그들이 따른) 잘못된 작업 지침, 그리고 작업을 수행하는 데 필요한 훈련 부족 등을 감안할 때 적절하게 행동하거나 적어도 이해할 만한 행동을 하였다. 또한 운영자들은 프로세스 컨트롤 시스템으로부터 거의 도움을 받지 못했지만 그들이 해야 하는 많은 작업에는 상당한 주의, 정밀성, 정신적인 노력, 프로세스 변동성(process dynamics)에 대한 깊은 이해, 그리고 지속적으로 변동하는 프로세스에 대한 빈번한 조정이 필요했다. 그러한 리스크들이 운영자들에게 제대로 전달되지 않았다.<br>관리자는 특이사항을 파악하고 프로세스를 중단하는 업무를 운영자에게 의존했지만 운영자들에게 이를 수행하는 데 필요한 정보와 훈련을 제공하지 않았다.<br><br>**권고사항:** 운영자는 할당받은 업무를 수행하기 위해 적절한 기술과 전문 지식을 갖춰야 하며 이러한 요건을 갖추도록 강제하는 사람이 있어야 한다. 운영자들이 스트레스가 많은 상황에서 적절한 결정을 내리는 데 필요한 정보 및 근로 조건 제공을 보장받기 위해 직무 분석 간 인적 요인에 대한 연구가 필요하다. 또한, 작업의 모든 단계에서 보다 나은 자동화된 지원이 제공되어야 하고, 기동(startup)과 같이 위험하다고 알려진 작업을 위한 교육이 제공되어야 하며, 작업 지침뿐만 아니라 그 지침을 생성하는 과정도 개선되어야 한다. |

| | |
|---|---|
| Plant Safety Management | **Role**:<br>(1) The safety analysis methods used were either not appropriate, not applied or were applied incorrectly. However, the methods used complied with the Shell requirements and with the minimum required by the Dutch regulators. Safety management did not consider some technical relevant information nor investigate how ethylbenzene reacting with the catalyst could cause an explosion. Safety management at Shell Moerdijk, as is common in many places, seems to have been largely ineffectual, with lots of activity, but much of it directed to minimal compliance with government regulation. A partial explanation for their behavior is that everyone believed that a reaction between ethylbenzene and the catalyst was impossible and that the start-up process was low risk.<br>(2) Although Shell's safety management system includes requirements for dealing with changes, the MOC procedures were not followed or implemented effectively. Risks resulting from changes made to the plant, the catalyst, the processes, and the procedures were not identified and managed.<br>(3) The number of leaks were used as the primary leading indicator of process safety. This practice is common in the petrochemical industry.<br>(4) Lessons from similar incidents at Nanhai and at Shell Moerdijk were not used to reduce risk.<br>(3) Proper oversight of the generation of work instructions was not provided, which allowed unsafe work instructions to be used by the operators.<br>**Recommendations**: While the problems specific to the explosions on 3 June 2014 should be fixed, there were a lot of weaknesses in the Shell Moerdijk safety management design and especially practices that were identified in the official Dutch Safety Agency accident report and in the CAST analysis. These need to be improved. In addition:<br>(1) Safety management at Shell Moerdijk needs to be made more effective. Safety engineering needs to be more than just going through the motions and minimally complying with standards.<br>(2) All work instructions should be reviewed for safety by knowledgeable people using information from the hazard analysis. [In this case, the hazard analysis was flawed too, but that is a different problem to fix.]<br>(3) MOC procedures must be enforced and followed. When changes occur, assumptions of the past need to be re-evaluated.<br>(4) Hazard analysis and risk assessment methods need to be improved.<br>(5) Better leading indicators of risk need to be identified and used.<br>(6) Procedures for incorporating and using lessons learned need to be established or improved. |
| Operations Management | **Role**:<br>(1) Operations management did not identify the flaws in the risk analyses performed or the procedures used for these risk analyses. The risk analyses complied with the minimal requirements of the Dutch regulatory authorities and apparently with the Shell requirements. |

| | |
|---|---|
| 플랜트 안전 관리 (Plant Safety Management) | **역할:**<br>(1) 사용된 안전 분석 방법이 적절하지 않았고 적용되지 않았거나 잘못 적용되었다. 그러나 사용된 방법은 쉘 요구사항과 네덜란드 규제기관이 요구하는 최소 기준을 준수하였다. 안전 관리 조직에서 일부 기술적 관련 정보를 고려하지 않았고 촉매제와 반응한 에틸벤젠이 어떻게 폭발을 일으킬 수 있었는지를 조사하지 않았다. 다른 많은 곳과 마찬가지로 쉘 뫼르딕의 안전 관리는 많은 활동에도 불구하고 대부분 효과가 없는 것처럼 보였고, 상당 부분이 정부 규제를 최소한으로 준수하는 방향으로 진행되었다. 그들의 행동에 대한 일부 설명에서는 모두가 에틸벤젠과 촉매제 간의 반응이 불가능하고 기동 프로세스의 리스크가 낮은 것으로 믿었기 때문이라고 하였다.<br>(2) 쉘의 안전관리 시스템은 변경사항에 대처하기 위한 요구사항을 포함하고 있지만 MOC 절차에서는 그러한 요구사항이 효과적으로 준수되거나 이행되지 않았다. 플랜트, 촉매제, 공정 및 절차의 변경으로 인해 발생한 리스크가 식별되고 관리되지 않았다.<br>(3) 공정 안전의 주요 선행지표로 누출 횟수가 사용되었다. 이것은 석유화학산업에서는 흔한 일이다.<br>(4) 유사한 사건인 난하이 및 쉘 뫼르딕 사건에서의 교훈이 리스크를 줄이는 데 사용되지 않았다.<br>(5) 작업 지침 생성에 대한 적절한 감독을 하지 않아서 운영자가 안전하지 않은 작업 지침을 따르게 되었다.<br><br>**권고사항:** 2014년 6월 3일 발생한 폭발에 대한 특정한 문제들은 반드시 해결되어야 하지만, 쉘 뫼르딕 안전관리 설계에 존재하는 많은 취약점도 반드시 개선되어야 한다. 특히 네덜란드 안전청 공식 사고 보고서 및 CAST 분석에서 확인된 관행에 많은 취약점이 있었다.<br>추가적으로:<br>(1) 쉘 뫼르딕의 안전관리를 보다 효과적으로 개선할 필요가 있다. 안전 엔지니어링은 단순히 형식적이거나 표준을 최소한으로 준수하는 것보다 더 많은 것을 수행할 필요가 있다.<br>(2) 모든 작업 지침은 지식이 풍부한 사람이 위험 분석 관련 정보를 활용하여 안전성 측면에서 검토해야 한다. [이 사건의 경우 위험 분석에도 결함이 있었는데 이는 개선되어야 할 또 다른 문제이다.]<br>(3) MOC 절차는 강제되고 준수되어야 한다. 변경사항이 있는 경우 기존의 가정을 재평가해야 한다.<br>(4) 위험 분석 및 리스크 평가 방법을 개선해야 한다.<br>(5) 더 나은 리스크 선행지표를 식별하고 사용해야 한다.<br>(6) 교훈을 반영 및 사용하는 절차를 수립하거나 개선해야 한다. |
| 운영 관리 (Operations Management) | **역할:**<br>(1) 운영 관리는 수행된 리스크 분석이나 리스크 분석의 절차에 존재하는 결함을 밝혀내지 못했다. 리스크 분석은 네덜란드 규제 당국의 최소 요구사항을 준수하였고 쉘 |

| | |
|---|---|
| | (2) Changes over time were not subjected to assessment in accordance with the MOC procedures.<br>(3) Work instructions were created by the operators without safety engineering oversight. They did not comply with the required Shell format for such work instructions and did not include important criteria for the job such as heating rate and nitrogen flow.<br>(4) Operations management decided to configure the process control system to control the plant during the normal production phase but not during non-production and maintenance phases. They did not think these activities were high risk and that manual operation would therefore suffice. The reasons for this decision are not in the accident report.<br>(5) They allowed two employees from different contractors to work in the adjacent unit during the start-up, probably because they did not believe that phase was dangerous.<br>(6) They did not assign operators to the start-up that had the qualifications required in the Safety Report. No reason is given in the accident report as to why this happened.<br>(7) They did not ensure that lessons learned from similar plants and at Shell Moerdijk in 1999 were incorporated in the design and operation of Unit 4800.<br>(8) They either did not follow MOC procedures or thought the procedures were unnecessary in this case. No information is in the report to determine this.<br>(9) They conducted internal Shell Moerdijk audits that did not detect any of the clear shortcomings in practices and procedures. Not enough information is provided to determine why the audits were ineffective.<br>**Recommendations**: (1) Establish and enforce proper MOC procedures. If changes occur, retest assumptions that could be affected by those changes. This implies that these assumptions must be recorded, leading indicators established for identifying when they may no longer be correct, and a process established for testing and responding to changes that might affect these assumptions.<br>(2) Do a thorough review of the Shell Moerdijk SMS with emphasis on why it was unable to prevent this accident. Major factors in this accident are related to basic activities that should have been controlled by the SMS.<br>(3) Update procedures to eliminate the causes of the accident such as lack of control and supervision of the work instruction creation and oversight processes, inadequate hazard analysis and risk assessment procedures, assignment of operators to perform the turnaround who did not have the required skills and expertise, inadequate use of lessons learned from the past, and audit procedures that did not identify the shortcomings before the accident.<br>(4) Improve the process control system to provide appropriate assistance to operators performing functions that are outside of normal production. |

| | |
|---|---|
| | 의 요구사항도 명백하게 준수하였다.<br>(2) 시간이 따른 변경사항은 MOC 절차에 의해 평가되지 않았다.<br>(3) 운영자가 안전 엔지니어링 감독 없이 작업 지침을 작성하였다. 그들이 작성한 작업 지침은 필요한 쉘 형식을 준수하지 않았고 가열율 및 질소 유량과 같은 작업의 중요한 기준을 포함하지 않았다.<br>(4) 운영 관리는 프로세스 컨트롤 시스템이 정상적인 생산 단계 동안에만 플랜트를 컨트롤하도록 구성하였으며, 비생산 및 유지보수 단계 동안에는 컨트롤 하지 않도록 구성하였다. 그들은 이러한 활동들이 리스크가 높지 않다고 생각하여 수동 작업만으로 충분할 것이라고 생각했다. 이러한 결정에 대한 근거는 사고 보고서에 명시되지 않았다.<br>(5) 기동 과정에서 두 명의 다른 계약업체 직원이 인접한 유닛에서 작업하도록 했는데 이는 해당 단계가 위험하지 않다고 생각했기 때문일 것이다.<br>(6) 안전 보고서에서 요구하는 자격을 갖춘 기동 운영자를 배정하지 않았다. 사고 보고서에는 왜 이런 일이 발생했는지에 대한 이유가 제시되지 않았다.<br>(7) 유사한 플랜트 및 1999년 쉘 뫼르딕에서의 교훈이 Unit 4800의 설계와 운영에 반영되도록 하지 않았다.<br>(8) MOC 절차를 따르지 않았거나 MOC 절차가 이 경우에는 불필요하다고 생각했다. 보고서에는 이러한 내용을 파악할 정보가 없다.<br>(9) 내부 쉘 뫼르딕 감사를 시행하였는데 이 감사에서는 관행 및 절차의 명확한 결점을 발견하지 못하였다. 보고서에서 감사가 왜 효과적이지 않았는지 파악하기 위한 충분한 정보가 제공되지 않는다.<br><br>**권고사항**: (1) 적절한 MOC 절차를 수립하고 시행한다. 변경사항이 있는 경우 그러한 변경에 영향을 받을 수 있는 가정을 다시 테스트한다. 이는 이러한 가정이 반드시 기록되어야 하는 것을 의미하고, 그러한 가정이 더 이상 맞지 않는 시점을 식별하기 위한 선행지표가 확립되어야 함을 의미하며, 이러한 가정에 영향을 미칠 수 있는 변경사항의 테스트 및 대응을 위한 프로세스가 확립되어야 함을 의미한다.<br>(2) 쉘 뫼르딕 SMS가 사고를 방지할 수 없었던 이유를 중점적으로 철저히 검토한다. 이번 사고의 주요 요인은 SMS가 통제했어야 할 기본적인 활동과 관련이 있다.<br>(3) 작업 지침 생성에 대한 컨트롤 및 감독(supervision)과 관리(oversight) 프로세스의 부족, 부적절한 위험 분석 및 리스크 평가, 턴어라운드(정비 유지보수)에 요구되는 기술 및 전문 지식이 없는 운영자 배정, 과거 교훈의 부적절한 사용 그리고 사고 이전에 단점을 식별하지 않은 감사와 같은 사고의 원인을 제거하기 위한 절차를 업데이트 한다.<br>(4) 프로세스 컨트롤 시스템을 개선하여 정상 생산 작업 이외의 업무를 수행하는 운영자를 적절하게 지원한다. |

| | |
|---|---|
| Shell Projects and Technology | **Role**: The design data provided to the licensees was not usable by those creating work instructions at the plants using the technology. The design had safety-critical design flaws that were not found in hazard analyses during the initial design phase and were not fixed after receiving information about serious problems in operations at some Shell plants. These design flaws include an inadequate number of temperature sensors and the use of pressure relief valves that could not handle the pressure that occurred. Unsafe and incomplete work instructions were approved by Shell Projects and Technology for the Unit 4800 turnaround at Shell Moerdijk.<br>Without more information about the operations at Shell Corporate, it is difficult to determine exactly why the unsafe control occurred. More questions than answers arise from the CAST analysis here, such as *Why were the design flaws introduced and how did they get through the design process? What type of hazard analysis is performed by Shell Projects and Technology (or used if it is produced by another group)? Why were identified design flaws not fixed after the incidents at Shell Moerdijk in 1999 and Nanhai in 2011? What other types of feedback (beyond incidents) is provided about the safety of their designs during operations in the Shell plants? What information about the safety aspects (hazards) of the plant design are passed from Shell Projects and Technology to the licensees of their designs? What information is included in the design book? Is the design data provided adequate for the licensees to create safe work instructions if engineers are writing the work instructions instead of operators? Did they not know who was going to be performing this task? Why did they approve unsafe work instructions that did not even follow the required Shell format? What information is provided in the Design Book specifically about start-up and the hazards of start-up? What types of hazard analysis are performed during the design process? What is the process for ensuring safety when changes are made? How are safety-related assumptions recorded and what are the triggers that initiate a re-analysis of these assumptions? What feedback do the designers receive about the operation of their designs?*<br><br>**Recommendations:** Fix the design features contributing to accident. Determine how these flaws got through the design process and improve the design and design review process. Improve the design book so that it is understandable by those who are writing the work instructions and contains all the information needed to safely operate installations of the licensed technology. Improve the work instruction review process by Shell Projects and Technology to ensure the instructions are complete and safe. Review and improve the hazard analysis process used by Shell Projects and Technology (or fix it elsewhere if this group does not do their own hazard analyses). |
| Corporate Safety Management | **Role**: There appears to have been a flawed view of the state of risk and the effectiveness of the safety management system in Shell plants. The flawed process model is most likely related to inadequate feedback (including audits and leading indicators). Again, many questions are raised in the CAST analysis that need to be answered in order to understand the role of corporate level safety management in the accident so that more effective safety management can be provided in the future. Almost nothing about safety management at the Corporate level is included in the accident report. |

| | |
|---|---|
| 쉘 프로젝트 앤 테크놀로지 (Shell Projects and Technology) | **역할:** 라이선스 보유자에게 제공된 설계 데이터는 플랜트에서 작업 지침을 생성하는 데 사용할 수 없었다. 이 설계는 초기 설계 단계의 위험 분석에서 발견되지 않은 안전 중요 설계 결함을 가지고 있었으며, 일부 쉘 플랜트에서 작업상의 심각한 문제에 대한 정보를 받은 후에도 수정되지 않았다. 이러한 설계 결함에는 온도 센서의 개수 부족과 압력 발생 시 그 압력을 처리하지 못하는 압력 완화 밸브의 사용이 포함된다. 쉘 프로젝트 앤 테크놀로지는 쉘 뫼르딕의 Unit 4800 턴어라운드(정비유지보수)에 대한 안전하지 않고 불완전한 작업 지침을 승인하였다.<br><br>쉘 기업의 운영에 대한 더 많은 정보가 없다면 안전하지 않은 컨트롤이 발생한 이유를 명확하게 파악하기 어렵다. CAST 분석에서는 답변보다 질문이 더 많이 제기된다. 예를 들어, *왜 설계 결함이 유입되었으며 그 결함이 설계 프로세스를 어떻게 통과했는가? 쉘 프로젝트 앤 테크놀로지에서는 어떤 유형의 위험 분석을 수행하는가? (또는 다른 그룹이 위험 분석을 한 경우 어떤 유형의 위험 분석을 사용하는가?) 1999년 쉘 뫼르딕 및 2011년 난하이 사건 이후 식별된 설계 결함은 왜 수정되지 않았는가? 쉘 플랜트의 작업 과정에서 설계 안전에 대한 (사건 이외의)피드백은 어떤 유형인가? 쉘 프로젝트 앤 테크놀로지가 설계 라이선스 보유자에게 전달한 플랜트 설계의 안전 측면(위험)에 대한 정보는 무엇인가? 설계서에 어떤 정보가 포함되어 있는가? 엔지니어가 운영자 대신 작업 지침을 작성하는 경우 라이선스 보유자가 안전한 작업 지침을 작성하기 위해 제공된 설계 데이터가 적절한가? 그들은 누가 이 업무를 수행하게 될지 몰랐는가? 그들은 요구되는 쉘 형식을 따르지 않은 안전하지 않은 작업 지침을 왜 승인했는가? 기동 및 기동의 위험에 대해 설계서에서 구체적으로 제공된 정보는 무엇인가? 설계 프로세스에서 수행된 위험 분석의 유형은 무엇인가? 변경사항이 있는 경우 안전을 보장하기 위한 프로세스는 무엇인가? 안전 관련 가정은 어떻게 기록되며 이러한 가정을 재분석하게 되는 트리거는 무엇인가? 설계자는 설계 작업에 대해 어떤 피드백을 받고 있는가? 등이 있다.*<br><br>**권고사항:** 사고에 기여하는 설계 특성을 수정한다. 설계 프로세스를 통해 이러한 결함이 어떻게 발생했는지 확인하고 설계 및 설계 검토 프로세스를 개선한다. 설계서를 개선하여 작업 지침 작성자가 그 설계서를 쉽게 이해할 수 있게 하고, 인증 받은 기술을 적용한 설비를 안전하게 운영할 수 있도록 모든 정보를 수록한다. 쉘 프로젝트 앤 테크놀로지의 작업 지침 검토 프로세스를 개선하여 그 지침이 완전하고 안전한지 확인한다. 쉘 프로젝트 앤 테크놀로지에서 사용하는 위험 분석 프로세스를 검토 및 개선한다(이 그룹이 위험 분석을 수행하지 않는 경우 위험 분석을 수행하는 다른 그룹에서 프로세스를 개선한다). |
| 기업 안전관리 (Corporate Safety Management) | **역할:** 쉘 플랜트의 리스크 상태 및 안전 관리 시스템의 효과 측면에 결함이 있었던 것으로 보인다. 결함 있는 프로세스 모델은 부적절한 피드백(감사 및 선행지표 포함)과 관련이 있을 가능성이 크다. 다시 말해 CAST 분석에서 제기된 많은 질문들은 사고와 관련된 기업 수준의 안전 관리 역할을 이해하기 위해 답변될 필요가 있다. 이는 향후 효과적인 안전 관리가 이루어질 수 있기 위함이다. 사고 보고서에는 기업 수준의 안전관리에 대한 내용은 거의 포함되어 있지 않다. |

| | |
|---|---|
| | **Recommendations**: Improve Shell safety audits. Review all risk assessment and hazard analysis processes and, in general, improve their approach to both safety analysis and safety management. Shell is not alone among the large oil companies in needing to update their methods. The petrochemical industry has too many accidents and incidents that are avoidable.<br>More specifically, the accident report says that Shell should "evaluate how risk analyses are performed and make changes. This should include procedures and policies requiring re-evaluation of earlier presumptions and assumptions. Conduct new risk analyses, put adequate measures in place and ensure that the team that performs these analyses has sufficient critical ability. Pay particular attention to assumptions based on risks that had previously been ruled out."<br>Evaluate and improve the corporate safety management system. Improve procedures for learning from process safety-related incidents. Create better feedback mechanisms (including audits and leading indicators) and procedures for learning from incidents. |
| Executive-Level Corporate Management | **Role**: Corporate management is responsible to ensure that an effective safety management system is created. Clearly typical policies of an effective safety management system were violated at both Shell Corporate and Shell Moerdijk. The group overseeing safety at the Shell corporate level was not effective. There is nothing included in the accident report about the assigned safety-related responsibilities for Corporate management. The Baker Panel report on the Texas City explosion found that BP corporate management did not have assigned responsibilities for safety, which instead was treated as a local responsibility. This abdication of responsibility (a practice promoted by HRO, which BP follows) was identified as a major contributor to the Texas City explosion [Baker 2007]. Is this a problem in general in the petrochemical industry?<br>There is also nothing included about context in the accident report that might explain why standard executive-level responsibilities for safety were not effectively carried out. There seems, however, to be a safety culture problem at Shell. Is this a problem in the Oil and Gas industry as a whole?<br>The accident report notes that the Safety Management System was integrated with the Business Management System at Shell Moerdijk. Was this also true at the corporate level? This is a very poor practice (and was a factor in the Deepwater Horizon accident). Safety risk assessments need to be kept separate from business risk assessments so that information is not hidden from high-level decision-makers.<br><br>**Recommendations**: Review the SMS design and determine why it did not prevent obvious violations of policy such as shortcomings in safety studies, management of change, learning from accidents, not following regulations (e.g., having experienced operators and following the format for work instructions). Determine why audits were not effective in finding such obvious violations of procedures. While it is possible that this was the first time such lapses have occurred, it is highly unlikely. Strengthen audit procedures, including identifying better leading indicators of |

| | |
|---|---|
| | **권고사항:** 쉘 안전 감사를 개선한다. 모든 리스크 평가 및 위험 분석 프로세스를 검토하고 안전 분석과 안전 관리에 대한 일반적 접근 방법을 개선한다. 대형 석유 기업들 중 접근 방법을 업데이트해야 하는 기업은 쉘뿐만이 아니다. 석유 화학 산업에서 피할 수 있는 사고와 사건은 너무나도 많다.<br><br>보다 구체적으로, 사고 보고서에서는 "리스크 분석 방법을 평가하고 변경한다. 이것은 초기의 추정 및 가정을 재평가하는 데 요구되는 절차와 정책을 포함해야 한다. 새로운 리스크 분석을 수행하고 적절한 조치를 취한다. 또한 이러한 분석을 수행하는 팀이 핵심 능력을 충분히 갖추도록 한다. 특히 이전에 누락된 리스크에 대한 가정을 주의해야 한다."라고 기술되어 있다.<br><br>기업의 안전 관리 시스템을 평가하고 개선한다. 프로세스 안전 관련 사건으로부터 학습하기 위한 절차를 개선한다. 더 나은 피드백 메커니즘(감사 및 선행지표 포함)과 사건으로부터 학습하기 위한 절차를 만든다. |
| 경영진의 기업 관리 (Executive-Level Corporate Management) | **역할:** 기업 경영진은 효과적인 안전 관리 시스템을 구축할 책임이 있다. 쉘 기업 및 쉘 뫼르딕에서는 효과적인 안전 관리 시스템의 전형적인 정책이 명백히 위반되었다. 쉘 기업 차원에서 수행한 안전 감독이 효과적이지 않았다. 기업 경영진의 안전 관련 책임에 대한 내용은 사고 보고서에 포함되어 있지 않다. 텍사스 시티 폭발에 대한 베이커 패널(BP, Baker Panel) 보고서에서는 BP의 기업 관리에서 안전에 대한 책임을 부여하지 않고 대신 지역 책임의 문제로 간주했다고 밝혔다. 이러한 책임(BP가 준수하는 HRO의 직무) 회피(abdication)가 텍사스 시티 폭발의 주요 원인으로 파악되었다[베이커 2007]. 이것이 석유 화학 산업에서 일반적으로 발생하는 문제인가?<br><br>경영진의 안전에 대한 일반적인 책임이 효과적으로 이행되지 않는 이유를 설명하는 컨텍스트도 사고 보고서에 포함되지 않았다. 그러나 쉘에서는 안전 문화의 문제로 보인다. 이것이 석유 및 가스 산업 전반에서 발생하는 문제인가?<br><br>사고 보고서에서는 쉘 뫼르딕의 안전 관리 시스템이 사업 관리 시스템과 통합되었다고 명시하고 있다. 이것은 기업 차원에서도 그러한가? 이것은 매우 잘못된 방식이다(그리고 딥워터 호라이즌 사고의 한 요인이었다). 안전 리스크 평가는 상위 수준의 의사결정권자에게 정보가 누락되지 않도록 사업 리스크 평가와 별도로 수행되어야 한다.<br><br>**권고사항:** SMS 설계를 검토하고 안전 연구의 취약점, 변경 관리 취약점 및 사고로부터의 학습 결점, 규정(예: 숙련된 운영자 보유 및 작업 지침의 형식 준수) 미준수와 같이 명백한 정책 위반을 방지하지 못한 이유를 파악한다. 감사에서 명백한 절차 위반을 효과적으로 발견하지 못한 이유를 파악한다. 그러한 과실이 처음 발생한 것일 수도 있지만 그럴 가능성은 거의 없다. 단순한 누출 횟수의 증가에 대한 선행지표가 아닌 리스크 증가에 대한 보다 나은 선행지표를 식별하고 감사 절차를 강화한다. 또한 안전 관리 시스템이 정상 상태를 이탈하여 리스크가 증가하는 시점을 식별하는 |

| | |
|---|---|
| | increasing risk than simply the number of leaks and create other forms of feedback to identify when the safety management system is drifting off course and risk is increasing. Establish better feedback channels to ensure that management of change procedures and corporate safety policy are being followed. |

| | |
|---|---|
| Catalyst Manufacturer | **Role**: The changes made in the catalyst were not pointed out to Shell, but they were included in a new safety information sheet. While the catalyst manufacturer cannot determine the impact of their changes on a customer, there should be some clear alert, other than simply changing information in a document, that changes have been made so that the customers are aware of them.<br><br>**Recommendations**: Change contractual relationships between Shell and its suppliers to ensure that potentially critical changes are communicated. Make changes within information sheets so they are clear and obvious. |

| | |
|---|---|
| Dutch Regulators | **Role**: The accident report implies that regulators gave Shell Moerdijk a pass on behavior that might have been labeled violations. Plant scenario deficiencies should have been considered a violation but were not. Scenarios were not up to date or were incomplete. Working under limited resources and time is difficult under any supervision model but system-level supervision has major limitations in ensuring public safety. The accident investigation showed many flaws in Shell Moerdijk operations safety management as defined and as implemented. So what is wrong with the supervision model that the regulators did not detect them?<br><br>**Recommendations**: Better supervision of the highest risk activities is needed, including turnarounds. Regulators need to oversee and ensure that strict procedures are being used for the most dangerous activities and that the safety management system is operating effectively and following its own rules. Operating under limited resources does not preclude doing something effective; it simply requires a more intelligent selection of activities that are performed. There is a need for better evaluation procedures and oversight of safety management system effectiveness. The regulators should rethink system-level supervision to ensure that they provide effective oversight in preventing accidents like the Shell Moerdijk explosions and fire. |
| Emergency Services | **Role**: Emergency services were mostly effective in carrying out their responsibilities, but some deficiencies, particularly in communication, were uncovered in the accident response.<br><br>**Recommendations**: Several deficiencies were uncovered in LCMS and NL-Alert communication protocols during this incident. While they did not lead to loss of life because of the nature of this accident, they could under other circumstances and what was learned from this case should be used to improve the system, including why many people used WhatsApp instead of LCMS and how the official system can incorporate those features. Accidents create an opportunity to look closely at the |

| | |
|---|---|
| | 다른 형태의 피드백을 생성한다. 변경 관리 절차 및 기업 안전 정책이 준수되도록 하기 위해 보다 나은 피드백 채널을 구축한다. |

| | |
|---|---|
| 촉매제 제조업체 (Catalyst Manufacturer) | **역할:** 쉘은 촉매제의 변경사항을 지적하지 않았지만 이는 새로운 안전 정보 기록에 포함되어 있었다. 촉매제 제조업체는 해당 변경사항이 고객에게 미치는 영향을 파악할 수는 없지만 단순히 문서에서 정보를 변경하는 것이 아닌 그 변경사항을 고객이 인지할 수 있도록 명확히 경고해야 한다.<br><br>**권고사항:** 쉘과 공급 업체 간의 계약 관계를 변경하여 잠재적으로 중요한 변경사항이 전달되도록 한다. 정보 기록을 변경하여 간결하고 명확하게 한다. |

| | |
|---|---|
| 네덜란드 규제기관 (Dutch Regulators) | **역할:** 사고 보고서에서는 규제기관이 쉘 뫼르딕의 위반으로 분류되었을 수도 있는 행동을 허가했다고 명시하고 있다. 플랜트의 시나리오 결함은 위반으로 간주되어야 했지만 그렇지 않았다. 시나리오는 최신 버전이 아니거나 완전하지 않았다. 제한된 자원 및 시간 하에서 업무를 수행하는 것은 모든 감독 모델에서 어려운 일이지만 시스템 수준의 감독은 공공 안전을 보장하는 데 있어 중대한 제한사항이 있다. 사고 조사에서는 쉘 뫼르딕 작업 안전 관리 정의 및 구현에 많은 결함이 있음을 보여주었다. 그렇다면 규제기관이 발견하지 못한 감독 모델의 문제점은 무엇인가?<br><br>**권고사항:** 턴어라운드(정비유지보수)를 포함하여 가장 높은 리스크 활동에 대해 보다 나은 감독이 필요하다. 규제기관은 가장 위험한 활동에 엄격한 절차가 사용되고 있으며 안전 관리 시스템이 효과적으로 운영되고 자체 규정을 준수하는지 감독하고 보장해야 한다. 제한된 자원 조건 하에서 운영한다고 효과적인 업무를 못하는 것은 아니다; 단지 수행할 활동에서 보다 현명한 선택을 필요로 한다. 안전 관리 시스템의 효과에 대한 보다 나은 평가 절차 및 감독이 필요하다. 규제기관은 쉘 뫼르딕 폭발 및 화재와 같은 사고를 방지하는 데 효과적인 감독을 위해 시스템 수준의 감독(supervision)을 재고해야 한다. |
| 비상 서비스 조직 (Emergency Services) | **역할:** 비상 서비스 조직은 대부분 책임을 효과적으로 수행하였지만 사고 대응과정의 의사소통에서 일부 문제점이 있었다.<br><br>**권고사항:** 이 사건에서는 LCMS와 NL-Alert 통신 프로토콜에서 몇 가지 결함이 발견되었다. 이 사고의 특성상 그것들이 인명 손실을 초래하지는 않았지만 다른 환경에서는 인명 손실이 발생할 수 있다. 많은 사람이 LCMS 대신 WhatsApp을 사용한 이유, 그 공식적인 시스템이 WhatsApp의 기능을 반영할 수 있는 방법 등 이번 사례를 통해 학습한 것들을 활용하여 시스템을 개선해야 한다. 사고는 비상시에 시스템의 실제 작동을 면밀하게 살펴볼 수 있는 기회와 놓쳐서는 안 될 학습 기회를 제공한다. |

| | |
|---|---|
| | actual operation of our systems in times of stress and provide a learning opportunity that should not be wasted. |

For the factors that spanned the entire control structure, not much information required for the CAST analysis was provided in the accident report. Some weaknesses are implied by what is included and some general recommendations can be derived.

| | |
|---|---|
| Safety Management System | Evidence of an overall inadequate safety control system and therefore safety management system in the report includes: unsafe situations were overlooked, internal procedures were not properly followed, lessons were not learned from previous incidents, incorrect assumptions about basic chemical reactions were not re-evaluated after evidence surfaced that they were incorrect, changes were not managed and controlled, inadequate hazard analysis and risk assessment procedures were used, recommendations from previous incidents and accidents were never implemented, and oversight of critical activities was missing. In summary, the Safety Management System at Shell Moerdijk did not prevent unsafe situations from being overlooked or internal procedures from not being followed. There is no information in the accident report about who created the SMS or who was responsible for ensuring that it was working properly.<br><br>**Recommendations**: The design of the entire safety management system should be evaluated and improved. In addition, the integration of the safety management system and the business management system should be carefully examined to ensure that hazard and risk-related information is being effectively communicated to decision makers and not stopped at inappropriately low levels. |
| Safety Information System | No information is provided about the safety information system but it appears that people were making decisions without having appropriate information.<br><br>**Recommendations**: The safety information system is so critical to the achievement of high safety that Shell and Shell Moerdijk should evaluate the existing system and perhaps redesign it. |
| Safety Culture | The accident report did not cover the safety culture in depth, but what is included seems to point to what has been labeled as a “compliance culture,” where the bulk of the effort is simply complying with standards and the requests of regulators and not proactively taking steps to improve safety. The accident report points to unsafe behavior that seems to imply safety was not a high priority, such as overlooking unsafe behavior and warnings, not adhering to internal procedures, not making changes after previous incidents, and not evaluating assumptions after changes occur.<br>The Hearts and Minds Safety Culture Program used by Shell has serious weaknesses. The “culture ladder” is vaguely defined (“we do a lot every time we have accidents”). Strangely, the company seems to be satisfied with their self-assessed current level in this program of *Calculative* (which is described in the |

전체 컨트롤 스트럭처의 여러 요소에 대해, CAST 분석에서 필요한 많은 정보가 사고 보고서에서 제공되지 않았다. 포함된 정보들이 몇 가지 약점들을 암시하고 있으며 이를 통해 일부 일반적인 권장 사항을 도출할 수 있다.

| | |
|---|---|
| 안전 관리 시스템 (Safety Management System) | 보고서에서 발견된 안전 컨트롤 시스템이 전반적으로 부적절하다는 증거는 다음과 같다: 안전하지 않은 상황을 간과함, 내부 절차를 제대로 따르지 않음, 이전 사건에서 교훈을 얻지 못함, 부정확한 증거가 드러난 후에도 기본적인 화학 반응에 대한 잘못된 가정을 재평가하지 않음, 변경사항을 관리 및 통제하지 못함, 부적절한 위험 분석 및 리스크 평가 절차를 사용함, 이전 사건 및 사고로부터의 권고사항이 시행되지 않음, 중요 활동에 대한 감독 누락 등. 요약하면 셸 뫼르딕의 안전 관리 시스템은 안전하지 않은 상황이 간과되거나 내부 절차를 준수하지 않는 것을 방지하지 못했다. 사고 보고서에는 SMS를 구축한 사람 또는 시스템이 제대로 동작하도록 하는 책임자에 대한 정보가 없다.<br><br>**권고사항:** 전체 안전 관리 시스템의 설계를 평가하고 개선해야 한다. 또한 안전 관리 시스템과 사업 관리 시스템의 통합을 면밀히 검토하여 위험 및 리스크 관련 정보의 전달이 부적절하게 하위 레벨에서 중단되지 않고 상위 레벨의 의사결정자에게 효과적으로 전달되도록 해야 한다. |
| 안전 정보 시스템 (Safety Information System) | 안전 정보 시스템에 대한 정보가 없었지만 사람들은 적절한 정보 없이도 결정을 내린 것으로 보인다.<br><br>**권고사항:** 안전 정보 시스템은 높은 안전성을 확보하는 데 매우 중요하므로 셸과 셸 뫼르딕은 기존 시스템을 평가해야 한다. 또한 기존 시스템을 재설계해야 할 수도 있다. |
| 안전 문화 (Safety Culture) | 사고 보고서에서는 안전 문화에 대해 깊이 다루지 않았으나 보고서에 포함된 “준수 문화”라고 불리는 것이 이를 의미하는 것 같다. “준수 문화”에서는 대부분의 노력을 단순히 표준 및 규제기관의 요구사항을 따르는 데에 쓰고 안전 개선을 위한 적극적인 조치는 취하지 않는다. 사고 보고서는 안전이 최우선 순위로 고려하지 않는 것처럼 보이는 행동을 지적한다. 그러한 행동에는 안전하지 않은 행동 및 경고 간과, 내부 절차 미준수, 사고 후에도 변경을 하지 않는 것, 변경 후 가정을 평가하지 않는 것 등이 있다.<br><br>셸이 사용하는 Hearts and Minds Safety Culture 프로그램은 심각한 취약점을 가지고 있다. “문화 단계(culture ladder)”는 애매하게 정의되어 있다(예: “우리는 사고가 날 때마다 많은 것을 한다.”). 이상하게도 회사는 이 *Calculative* 프로그램에서 자체 평가한 현재 수준(사고 보고서에 “필수” 수준이라고 명시된)에 만족하고 있는 것처럼 보였지만 그 수준조차 달성되지 못한 것 같다(심지어 소위 말하는 “하위” 수준도 아님). |

| | |
|---|---|
| | accident report as the “required” level), but even that level does not seem to have been achieved(nor even the so-called “lower” levels).<br><br>**Recommendations**: Shell Moerdijk and Shell Corporate should do a thorough study of their safety culture and determine why it was not strong enough to prevent the events in 2014. |
| Communication and Coordination | **Recommendations**: Communication channels, especially feedback channels, should be examined to determine whether they are effectively conveying the information necessary to operate safely. An important part of this includes performing a human factors analysis of the information provided to the operators and the potential for human errors created by the design of the process and particularly by the design of the process control system. |
| Management of Change | **Role**: A large number of both planned and unplanned changes contributing to the accident were not assessed for risk.<br><br>**Recommendations**: The Management of Change procedures should be evaluated to determine why they were not effective in this case and appropriate improvements implemented. |

| | |
|---|---|
| | **권고사항:** 쉘 뫼르딕과 쉘 기업은 그들의 안전 문화를 철저히 연구하여 안전 문화가 2014년에 발생한 사고를 방지하지 못한 이유를 파악해야 한다. |
| 의사소통 및 조정 (Communication and Coordination) | **권고사항:** 의사소통 채널, 특히 피드백 채널이 안전하게 작동하기 위해 필요한 정보를 효과적으로 전달하고 있는지 조사해야 한다. 이 조사에서 중요한 부분은 운영자에게 제공되는 정보의 인적 요인 분석, 프로세스 설계, 특히 프로세스 컨트롤 시스템의 설계에 의해 생성되는 인적 오류 가능성이 포함된다. |
| 변경 관리 (Management of Change) | **역할:** 사고에 기여하는 계획되거나 계획되지 않은 많은 변경 사항들에 대해 리스크 평가가 이루어지지 않았다.<br><br>**권고사항:** 이 사례에서 변경절차 관리가 효과적이지 않았던 이유와 적절한 개선이 이루어졌는지를 파악하기 위해 변경절차 관리를 평가해야 한다. |

# Appendix C: The Bad Apple Theory of Accident Causation

Blaming workers in accident investigation is based partially on the outdated and erroneous "bad apple" theory.[28] This concept says that there are a certain number of "bad apples" or a few people in a system that are responsible for most of the accidents. Most everything would be safe, in this view, if it were not for a few unreliable humans.

The concept goes back to 1925 when both German and British psychologists were convinced they would solve the safety problem by identifying and getting rid of the bad apples in an organization. They used statistical analysis over 50 years to determine that there were a cohort of "accident-prone" workers. These were people with personal characteristics that, they claimed, predisposed them to making errors and thus precipitating accidents. The data seemed to imply that a small percentage of people is responsible for a large percentage of accidents. If those people were removed, the system would become much safer.

The bad apple theory existed until WW II, when the complexity of the systems we were creating and that humans had to work within, started to increase dramatically. The theory was finally put to rest in 1951 by two statisticians, Arbous and Kerrich.

The theory did not work because of a major statistical flaw in the argument. For the accident-prone or bad apple theory to work, the risk of error and accidents must be equal across every system. But, of course, it is not. Newer views of accident causation conclude that personal characteristics do not carry as much explanatory power for why accidents occur as context does.

> *'When faced with a human error problem you may be tempted to ask 'Why didn't they watch out better? How could they not have noticed?' You think you can solve your human error problem by telling people to be more careful, by reprimanding the miscreants, by issuing a new rule or procedure. They are all expressions of the 'Bad Apple Theory' where you believe your system is basically safe if it were not for those few unreliable people in it. This old view of human error is increasingly outdated and will lead you nowhere.'* – Sidney Dekker*, A Field Guide to Understanding Human Error*, 2002.

The bad apple theory is especially prevalent in medicine, but it permeates almost every industry in the form of argument that most accidents are caused by human operators. If, for example, one posits that 5% of bad doctors cause most accidents, then simply identifying and getting rid of the doctors who get the most complaints and are involved in adverse events should drastically reduce medical error. Unfortunately, it does not. It may simply get rid of a group of doctors who do the really difficult, tricky work (e.g., some oncological cases with a negative prognosis).

More generally, if there are system features that are likely to induce human mistakes under some circumstances (e.g., poor facilities with limited resources and financial and other stresses), then swapping the humans involved, but not changing the system features that are creating the erroneous behavior, will have little impact on the accident rate. We know now that the design of systems has the potential to create various classes of errors such as mode confusion or, conversely, to reduce them. Surprisingly, most humans don't realize they are being influenced by their environment. Think about how you are fooled by optical illusions, even when you know they are there.

---

[28] Much of the information in this appendix comes from Sidney Dekker. We wrote an editorial together on the systems approach to medicine (Dekker, S. and Leveson, N. The systems approach to medicine: Controversy and misconceptions, *British Medical Journal: Quality and Safety*, 2014 and "The bad apple theory won't work", British Medical Journal: Quality and Safety, Nov. 2014). Dekker also wrote about the "new view" of human error and the "bad apple" theory in his 2002 book *The Field Guide to Understanding Human Error,* Ashgate Publishers, 2006.

# 부록 C: 사고 원인에 대한 썩은 사과(Bad Apple) 이론

사고 조사에서 작업자들을 비난하는 것은 일부 낡고 잘못된 "썩은 사과" 이론[28]에 기반하고 있다. 이 개념에 따르면 대부분의 사고 원인이 되는 시스템에 일부 "썩은 사과들" 또는 소수의 사람들이 있다. 이 관점에서는 그 신뢰할 수 없는 몇몇 사람이 없었다면 거의 대부분 안전했을 것이다.

이 개념은 1925년으로 거슬러 올라가는데, 그 당시 독일과 영국의 심리학자들은 한 조직에서 썩은 사과를 식별하고 제거함으로써 안전 문제를 해결할 것이라고 확신하였다. 그들은 50년 동안의 통계적 분석을 기반으로 "사고 경향성(accident-prone)" 작업자 집단(cohort)이 있다고 판단했다. 그들이 주장한 이 집단의 사람들은 실수를 저지르고 사고를 유발하는 개인적인 성향을 가진 사람들이었다. 이 데이터는 소수의 사람들이 대부분의 사고에 책임이 있음을 암시하는 것처럼 보였다. 만약 그 사람들이 제외된다면 시스템은 훨씬 더 안전해졌을 것이다.

썩은 사과 이론은 제2차 세계 대전 당시까지 존재하였으며, 그 시기에 개발하는 시스템의 복잡성이 급격하게 증가하기 시작했으며 사람이 시스템 내부에서 함께 일해야만 했다. 이 이론은 1951년 아르보스(Arbous)와 케리치(Kerrich) 두 명의 통계학자에 의해 마침내 폐기되었다.

썩은 사과 이론은 중대한 통계적 결함 때문에 논쟁에서는 활용할 수 없었다. 사고 경향성 또는 썩은 사과 이론이 활용되려면 모든 시스템에서 오류 및 사고에 대한 리스크가 동일해야 한다. 그러나 물론 그렇지 않다. 사고 인과관계에 대한 새로운 관점에서는 개인적 성향이 주어진 상황(context)에 기반한 설명만큼 사고가 발생하는 이유를 강력하게 설명할 수 없다고 결론 내리고 있다.

> *'당신은 인적 오류 문제에 직면했을 때 '왜 그들은 좀 더 주의하지 않았을까? 어떻게 그들은 알아차리지 못했을까?'라고 묻고 싶을 것이다. 당신은 사람들에게 좀 더 조심하라고 말하고, 잘못한 사람을 질책하고, 새로운 규칙이나 절차를 배포함으로써 인적 오류 문제를 해결할 수 있다고 생각한다. 이것들은 모두 '썩은 사과 이론'의 표현이며 소수의 신뢰할 수 없는 사람들이 없었다면 시스템이 기본적으로 안전하다고 믿을 수 있다는 것이다. 인적 오류에 대한 이 오래된 견해는 점점 시대에 뒤처지고 있으며 아무 도움이 되지 못할 것이다.' – 시드니 데커*(Sidney Dekker), *인적 오류 이해를 위한 현장 가이드,* 2002.

썩은 사과 이론은 특히 의학계에 널리 퍼져 있지만 거의 모든 다른 산업에서도 대부분의 사고가 운영자(human operator)에 의해 발생한다는 주장의 형태로 퍼져 있다. 예를 들어 형편없는 의사의 5%가 대부분의 사고를 일으킨다고 한다면 컴플레인을 많이 받고 부정적인 사고와 관련이 많은 의사를 식별하여 없애면 의료 과실은 감소해야 한다. 불행하게도 그렇지 않으며 실제로는 어렵고 까다로운 업무를 수행하는 의사 그룹을 없애게 될 수도 있다(예: 예후가 좋지 않은 일부 암 연구 사례).

보다 일반적으로 보면, 특정 상황에서(예: 한정된 자원, 재정 및 기타 스트레스가 있는 열악한 시설) 시스템의 특성이 사람의 실수를 유도할 가능성이 있는 경우 관련자들을 교체하더라도 잘못된 행동을 유발하는 시스템 특성을 바꾸지 않는 한 사고율에 거의 영향을 미치지 않을 것이다. 우리는 이제 이러한 시스템의 설계가 모드 혼동과 같은 다양한 종류의 오류를 생성하거나, 또는 반대로 오류를 감소시킬 가능성이 있음을 알고 있다. 놀랍게도 대부분의 사람들은 자신이 환경에 영향을 받고 있다는 것을

[28] 이 부록의 많은 정보는 시드니 데커(Sidney Dekker)의 저서에서 인용하였다. 우리는 의학에 대한 시스템적 접근에 대해 사설을 함께 명시하였다(Dekker, S. and Leveson, N. The systems approach to medicine: Controversy and misconceptions, British Medical Journal: Quality and Safety, 2014 and "The bad apple theory won't work", British Medical Journal: Quality and Safety, Nov. 2014). 또한 데커는 그의 2002년 저서인 인적 오류 이해를 위한 현장 가이드(에쉬게이트(Ashgate) 출판사, 2006)에서 인적 오류에 대한 "새로운 견해(new view)"와 "썩은 사과(bad apple)"이론에 대해 기술하였다.

As a simple physical example, consider the designs for a stove top shown in Figure C.1 from Don Norman's *The Design of Everyday Things* (Basic Books, 2013). These designs, which are common even today, require labels to connect the knobs with the cooking surfaces. Even after fairly extensive use, one may still need to read the labels to make the proper association or, if in a hurry, operate the wrong knob.

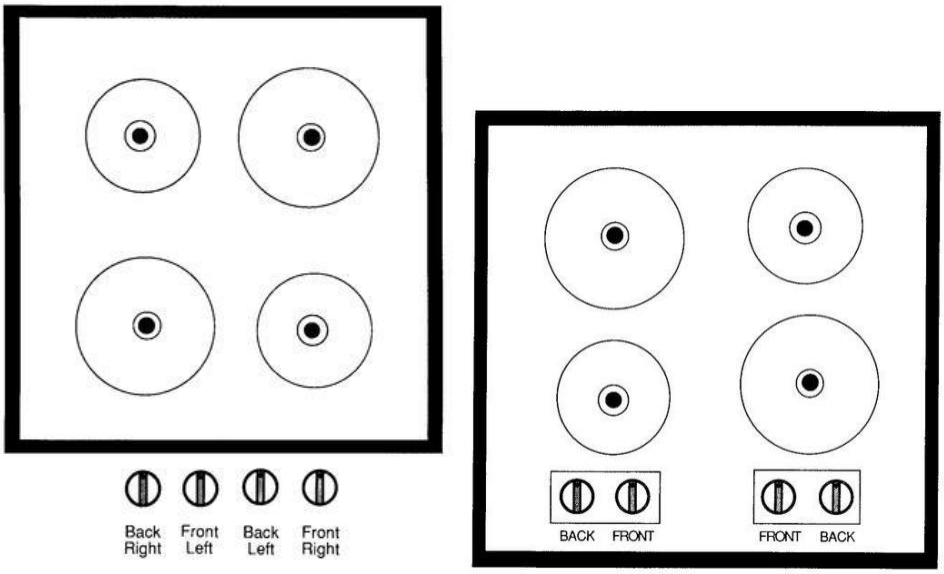



**Figure C.1**: Two designs of an error-prone stove top (Adapted from Don Norman, The Design of Everyday Things, Basic Books, 2013).

The designs in Figure C.2 eliminates most of these errors and, in fact, the need for labels is eliminated.

The examples of physical designs that induce human errors (or at least do not prevent them) shown in Figure C.1 are relatively simple to avoid in system design (which does not explain why so many stove tops today still use the error-prone design). But the problem is greatly exacerbated when cognitively complex decision making is required by operators. Most of our systems today require humans to work with computers and other complex designs that can more easily create an incorrect mental model on the part of the human about the state of the system or the state of the automation. Blaming the human, then, for erroneous behavior without looking at why that behavior occurred does nothing to reduce accidents due to the flawed system design. Pilots today, for example, are doing the wrong thing in a certain situation because of factors like inconsistent behavior of the automation, misunderstanding about how the automation is designed, confusion about the current mode of the aircraft or its automation, etc. Identifying these error-inducing design features during accident causal analysis, rather than simply stopping with "operator error," will allow us to improve safety in both current systems and in our future designs.

인식하지 못한다. 심지어 착시현상이 있음을 알고 있더라도 어떻게 그것에 속게 되었는가에 대해 생각해봐야 한다.

간단한 물리적 예로 도널드 노먼(Don Norman)의 *The Design of Everyday Things* (Basic Books, 2013)의 그림 C.1에 표시된 스토브(stove) 상단의 설계를 고려해보자. 오늘날에도 일반적으로 사용되는 이러한 설계에는 노브(knob)와 각 화구를 연결하는 명칭이 필요하다. 이 설계는 매우 널리 사용하고 있는 것이지만 라벨을 읽어야만 맞는 연결을 찾을 수 있고 급한 경우에는 잘못된 노브를 작동시킬 수 있다.

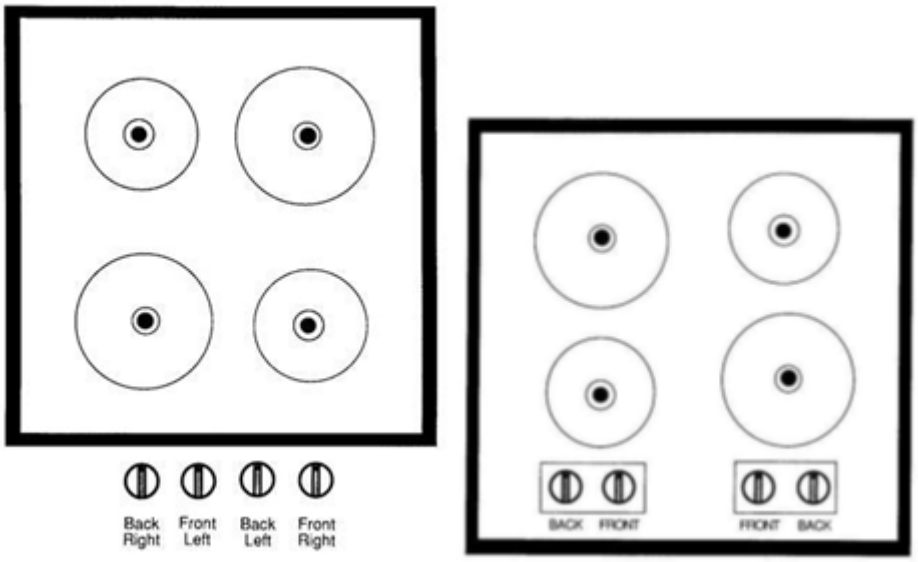



그림 C.1: 오류가 발생하기 쉬운 두 가지 스토브 상단 설계 (Don Norman, The Design of Everyday Things, Basic Books에서 인용, 2013).

그림 C.2의 설계는 이러한 오류의 대부분을 없애며 실제로 라벨의 필요성이 없어진다.

그림 C.1에 나타난 인적 오류를 유발하는(또는 적어도 그 오류를 방지하지 않는) 물리적 설계의 예는 시스템 설계에서 비교적 간단하게 피할 수 있다(오늘날의 많은 스토브 상단이 오류를 자주 발생시키는 설계를 사용하고 있는데 그 이유는 별도로 설명하지 않는다). 그러나 운영자가 복잡한 의사결정을 해야 한다면 문제가 크게 악화된다. 오늘날 대부분의 시스템은 사람이 컴퓨터 또는 다른 복잡한 설계와 상호작용하도록 요구한다. 그런데 이 복잡한 설계는 자동화 상태에서의 사람의 역할에 대한 잘못된 멘탈 모델을 갖게 할 가능성이 높다. 잘못된 행동에 대해 왜 그런 행동을 했는지 살펴보지 않고 사람을 비난하는 것은 결함 있는 시스템 설계로 인한 사고를 줄이는 데 아무런 도움이 되지 않는다. 예를 들어, 오늘날의 조종사들은 특정한 상황에서 잘못된 행동을 하고 있는데 이는 자동화의 일관성 없는 동작, 자동화 설계 방법에 대한 오해, 항공기의 현재 모드 또는 자동화에 대한 혼란 등과 같은 요인 때문이다. 단순히 “운영자 오류”로 멈추는 것이 아닌 사고 원인 분석과정에서 이러한 오류를 유발하는 설계 특성을 식별함으로써 현재 시스템 및 미래의 설계 모두에서 안전을 향상시킬 수 있다.

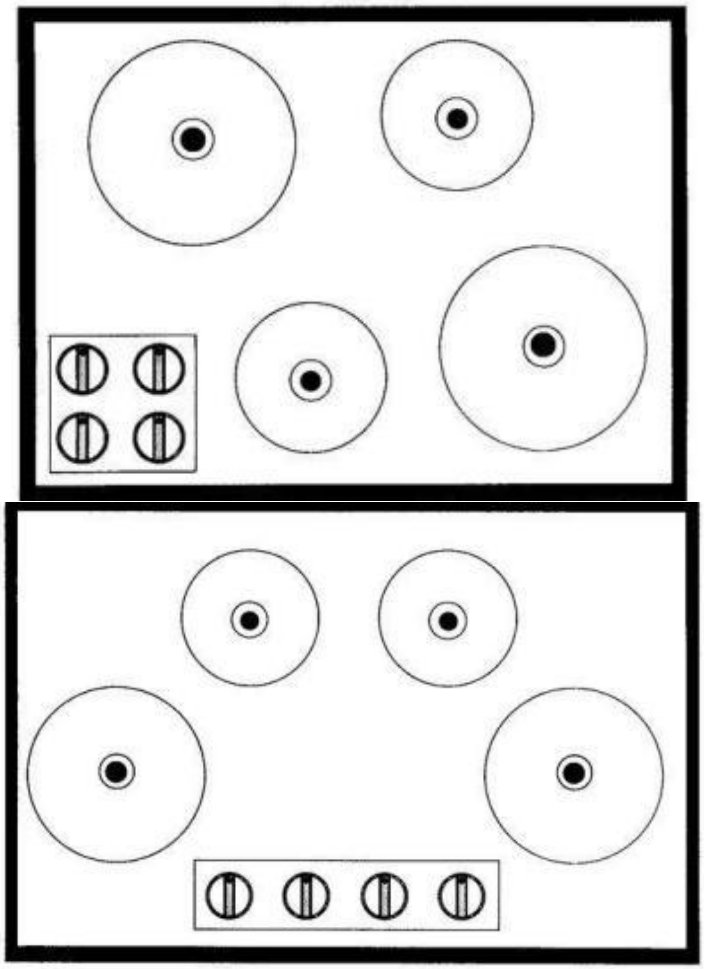


**Figure C.2**: Less error-prone designs (Adapted from Don Norman, The Design of Everything Things, Basic Books, 2013).

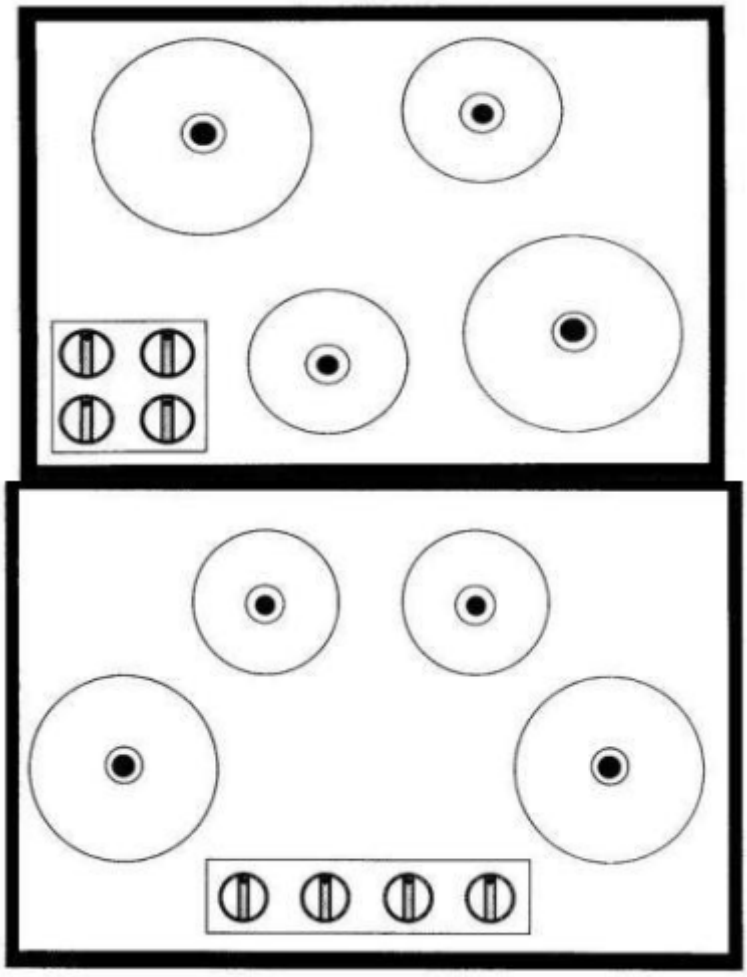


**그림 C.2:** 오류가 자주 발생하지 않는 설계 (Don Norman, The Design of Everything Things, Basic Books에서 인용, 2013).

# Appendix D: Factors to Consider When Evaluating the Role of the Safety Control Structure in the Loss

The list below (from *Engineering a Safer World*, Chapter 13) can be used in identifying inadequate controls and control structures when performing incident and accident analysis. It is not meant to be exhaustive and may need to be supplemented for specific industries and safety programs.

This list contains general responsibilities and does not indicate how they should be assigned. Appropriate assignment of the responsibilities to specific people and places in the organization will depend on the management structure of each organization. Each general responsibility may be separated into multiple individual responsibilities and assigned throughout the safety control structure, with one group actually implementing the responsibilities and others above them supervising, leading or directing, or overseeing the activity. Of course, each responsibility assumes the need for associated authority and accountability, as well as the controls, feedback, and communication channels necessary to implement the responsibility.

## General Management

- Provide leadership, oversight, and management of safety at all levels of the organization.
- Create a corporate or organizational safety policy. Establish criteria for evaluating safety-critical decisions and implementing safety controls. Establish distribution channels for the policy. Establish feedback channels to determine whether employees understand it, are following it, and whether it is effective. Update the policy as needed.
- Establish corporate or organizational safety standards and then implement, update, and enforce them. Set minimum requirements for safety engineering in development and operations and oversee the implementation of those requirements, including any contractor activities. Set minimum physical and operational standards for hazardous operations.
- Establish incident and accident investigation standards and ensure recommendations are implemented and effective. Use feedback to improve the standards.
- Establish management of change requirements for evaluating all changes for their impact on safety, including changes in the safety control structure. Audit the safety control structure for unplanned changes and migration toward states of higher risk.
- Create and monitor the organizational safety control structure. Assign responsibility, authority, and accountability for safety.
- Establish working groups.
- Establish robust and reliable communication channels to ensure accurate management risk awareness of the development system design and the state of the operating process. These channels should include contractor activities.
- Provide physical and personnel resources for safety-related activities. Ensure that those performing safety-critical activities have the appropriate skills, knowledge, and physical resources.
- Create an easy-to-use problem reporting system and then monitor it for needed changes and improvements.
- Establish safety education and training for all employees and establish feedback channels to determine whether it is effective along with processes for continual improvement. The education should include reminders of past accidents and causes and input from lessons learned and trouble reports. Assessment of effectiveness may include information obtained from knowledge assessments during audits.

# 부록 D: 손실에서 안전 컨트롤 스트럭처의 역할을 평가할 때 고려해야 할 요소

아래의 내용(*Engineering a Safer World*, 13장에 있음)은 사건 및 사고 분석 수행 시 부적절한 컨트롤과 컨트롤 스트럭처를 식별하는 데에도 사용할 수 있다. 컨트롤 스트럭처는 모든 것을 망라한 것은 아니며 특정 산업 및 안전 프로그램에 대해서는 보완이 필요할 수도 있다.

이 목록에는 일반적인 책임이 포함되어 있으며 책임을 할당하는 방법을 명시하고 있지는 않다. 각 조직의 관리 구조에 따라 특정 사람과 지위에 대한 적절한 책임 할당이 달라진다. 각각의 일반적인 책임은 다수의 개별 책임으로 나누어져 안전 컨트롤 스트럭처 전반에 걸쳐 할당되는데 한 그룹에서 실제로 책임을 이행하고 그 상위의 다른 그룹에서 이를 감독, 지도 또는 지시하거나 활동을 전체적으로 감독한다. 물론, 각 책임에는 책임 이행에 필요한 컨트롤, 피드백, 의사소통 채널뿐만 아니라 관련된 통제권한과 의무가 필요하다고 가정한다.

## 일반적인 관리(General Management)

- 조직의 모든 수준에서 리더십, 감독, 안전 관리를 제공한다.
- 기업 또는 조직의 안전 정책(safety policy)을 수립한다. 안전 필수 결정을 평가하고 안전 컨트롤을 구현하기 위한 기준을 수립한다. 정책의 배포 채널을 구축한다. 직원이 정책을 이해하고 있는지, 따르고 있는지, 효과적인지를 확인하기 위한 피드백 채널을 구축한다. 필요 시 정책을 업데이트 한다.
- 기업 또는 조직의 안전 표준(safety standard)을 수립하고 이행, 업데이트 및 강제한다. 개발과 운영에서의 안전 엔지니어링에 대한 최소 요구사항을 설정하고 그러한 요구사항(계약자의 활동 포함)의 이행을 감독한다. 위험한 작업을 위한 최소한의 물리적, 운영 표준을 설정한다.
- 사건 및 사고 조사 표준을 수립하고, 권고사항을 시행하고 효과적인지 여부를 확인한다. 피드백을 활용하여 표준을 개선한다.
- 안전에 영향을 미치는 모든 변경사항을 평가하기 위한 변경 요구사항 관리 체계를 수립한다. 변경 요구사항에는 안전 컨트롤 스트럭처의 변경도 포함한다. 안전 컨트롤 스트럭처에 대한 계획되지 않은 변경이나 리스크가 높은 상태로 진입하는 것을 감사(audit)한다.
- 조직의 안전 컨트롤 스트럭처를 만들고 모니터링 한다. 안전을 위한 책임, 통제권한 및 의무를 할당한다.
- 워킹 그룹을 만든다.
- 견고하고 신뢰할 수 있는 의사소통 채널을 구축하여 개발 시스템 설계 및 운영 프로세스 상태의 관리 리스크를 정확히 인식할 수 있도록 한다. 이러한 채널에는 계약자의 활동이 포함되어야 한다.
- 안전 관련 활동을 위한 물리적, 인적 자원을 제공한다. 안전 필수 활동을 수행하는 사람이 적절한 기술, 지식 및 물리적 자원을 갖추고 있는지 확인한다.
- 사용하기 쉬운 문제 보고 시스템(problem reporting system)을 만들고 필요한 변경사항이나 개선사항이 있는지 모니터링 한다.
- 모든 직원을 대상으로 안전 교육 및 훈련을 실시하고, 프로세스의 지속적인 개선을 위해 효과를 확인하기 위한 피드백 채널을 구축한다. 교육 내용에는 과거 사고를 상기시키는 것, 교훈과 문제 보고서로부터 얻은 원인이나 정보를 포함해야 한다. 효과의 평가에는 감사 과정에서의 지식 평가 정보가 포함될 수 있다.
- 안전 관련 기술적 의사 결정이 비용 및 일정 등의 계획에 따른 고려사항과는 독립적임을 보장하기

- Establish organizational and management structures to ensure that safety-related technical decision making is independent from programmatic considerations, including cost and schedule.
- Establish defined, transparent, and explicit resolution procedures for conflicts between safety-related technical decisions and programmatic considerations. Ensure that the conflict resolution procedures are being used and are effective.
- Ensure that managers who are making safety-related decisions are fully informed and skilled. Establish mechanisms to allow and encourage all employees (including front-line operators) and contractors to contribute to safety-related decision making.
- Establish an assessment and improvement process for safety-related decision making.
- Create and update the organizational safety information system.
- Create and update safety management plans.
- Establish communication channels, resolution processes, and adjudication procedures for employees and contractors to surface complaints and concerns about the safety of the system or parts of the safety control structure that are not functioning appropriately. Evaluate the need for anonymity in reporting concerns.

## Development

- Implement special training for developers and development managers in safety-guided design and other necessary skills. Update this training as events occur and more is learned from experience. Create feedback, assessment, and improvement processes for the training.
- Create and maintain the hazard log. Establish and maintain documentation and tracking of hazards and their status.
- Establish working groups.
- Design safety into the system using system hazards and safety constraints. Iterate and refine the design and the safety constraints as the design process proceeds. Ensure the system design includes consideration of how to eliminate or reduce contextual factors that cause or contribute to unsafe operator behavior that, in turn, contributes to system hazards. Distraction, fatigue, etc. are risk factors resulting from design that is dependent on humans performing in a way the designer imagined they would rather than behaving as normal humans would in such situations.
- Document operational assumptions, safety constraints, safety-related design features, operating assumptions, safety-related operational limitations, training and operating instructions, audits and performance assessment requirements, operational procedures, and safety verification and analysis results. Document both what and why, including tracing between safety constraints and the design features to enforce them.
- Perform high-quality and comprehensive hazard analyses and make these available and usable when safety-related decisions need to be made, starting with early decision making and continuing through the system's life. Ensure that the hazard analysis results are communicated in a timely manner to those who need them. Establish a communication structure that allows communication downward, upward, and sideways (i.e., among those building subsystems). Ensure that hazard analyses are updated as the design evolves and test experience is acquired.
- Train engineers and managers to use the results of hazard analyses in their decision making.
- Maintain and use hazard logs and hazard analyses as experience is acquired. Ensure communication of safety-related requirements and constraints to everyone involved in development.
- Gather lessons learned in operations (including accident and incident reports) and use them to improve the development processes. Use operating experience to identify flaws in the development of safety controls and implement improvements.

위한 조직 및 관리 구조를 구축한다.

- 안전 관련 기술적 결정과 계획에 따른 고려사항 간의 갈등에 대해, 규정되고 명백하며 명시적인 해결 절차를 수립한다. 갈등 해결 절차가 실제로 사용되고 있고 효과적인지를 확인한다.
- 안전 관련 결정을 내리는 관리자가 충분한 정보를 가지고 있고 숙련된 사람인지 확인한다. 안전 관련 의사 결정에 모든 직원(일선 운영자 포함) 및 계약자가 참여하도록 독려하기 위한 메커니즘을 수립한다.
- 안전 관련 의사 결정을 위한 평가 및 개선 프로세스를 수립한다.
- 조직의 안전 정보 시스템(SIS)을 만들고 업데이트 한다.
- 안전 관리 계획을 만들고 업데이트 한다.
- 의사소통 채널, 해결 프로세스, 판정(adjudication) 절차를 수립하여 직원 및 계약자가 시스템 안전 또는 적절하게 기능하지 못하는 안전 컨트롤 스트럭처 부분에 대한 불만과 우려를 제기할 수 있도록 한다. 우려 보고에 대해 익명성이 필요한지 평가한다.

## 개발(Development)

- 개발자와 개발 관리자를 대상으로 안전이 고려된 설계(safety-guided design) 및 다른 필요한 기술에 대한 특별 훈련을 실시한다. 이벤트가 발생하거나 경험을 통해 더 많은 것을 배울 때마다 이 훈련 프로그램을 업데이트 한다. 이러한 훈련의 피드백과 평가, 개선 절차를 만든다.
- 위험 로그를 작성하고 유지관리한다. 위험 및 위험의 상태에 대해 문서화하고 추적성을 수립하여 유지관리 한다.
- 워킹 그룹을 만든다.
- 시스템 위험과 안전 제약사항을 활용하여 시스템에 안전을 설계한다. 설계가 진행됨에 따라 설계와 안전 제약사항을 반복하여 상세화한다. 운영자의 안전하지 않은 행동을 유발하거나, 그러한 행동에 기여하여 결국 시스템 위험을 야기하는 컨텍스트적(contextual) 요인을 제거 또는 감소시키는 방법에 대한 고려사항이 시스템 설계에 포함되도록 한다. 특정 상황에서 일반적인 사람들이 행동하는 방식으로 설계하지 않고 설계자가 상상한 사람들의 행동 방식에 의존하여 설계하면 주의산만(distraction), 피로(fatigue) 등의 리스크 요인이 발생할 수 있다.
- 운영상의 가정, 안전 제약사항, 안전 관련 설계 기능, 동작 가정, 안전 관련 운영상의 제약, 훈련 및 운영 지침, 감사 및 성과 평가 요구사항, 운영 절차, 안전 검증(verification) 및 분석 결과를 문서화한다. 안전 제약사항과 그것을 강제하기 위한 설계 특징 간의 추적성을 포함하여, 무엇(what)과 왜(why)에 대한 사항을 문서화한다.
- 초기 의사 결정부터 시스템 수명주기 전체에 이르기까지 지속적으로 고품질의 포괄적인 위험 분석을 수행하여 안전 관련 결정이 내려질 때 그 위험 분석 결과를 사용할 수 있게 한다. 위험 분석 결과가 그것을 필요로 하는 사람들에게 적시에 전달되도록 한다. 의사소통이 아래쪽, 위쪽, 옆쪽(즉, 서브시스템간에)으로 가능하도록 의사소통 구조를 구축한다. 설계가 진화되고 테스트 경험이 축적됨에 따라 위험 분석 결과를 업데이트 한다.
- 엔지니어와 관리자가 위험 분석 결과를 의사 결정에 사용할 수 있도록 훈련한다.
- 경험이 축적됨에 따라 위험 일지와 위험 분석 결과를 유지관리하고 활용한다. 안전 관련 요구사항과 제약사항을 개발과 관련된 모든 사람에게 전달한다.
- 운영 과정에서의 교훈(사고 및 사건 보고서 포함)을 모아서 개발 프로세스를 개선하는 데 사용한다. 운영 경험을 활용하여 안전 컨트롤의 개발 시 결함을 식별하고 개선한다.

## Operations

- Create an operations safety management plan
- Develop special training for operators and operations management to create needed skills and update this training as events occur and more is learned from experience. Create feedback, assessment, and improvement processes for this training. Train employees to perform their jobs safely, understand proper use of safety equipment, and respond appropriately in an emergency.
- Establish working groups.
- Maintain and use hazard logs and hazard analyses during operations as experience is acquired.
- Ensure all emergency equipment and safety devices are operable at all times during hazardous operations. Before safety-critical, non-routine, potentially hazardous operations are started, inspect all safety equipment to ensure it is operational, including the testing of alarms.
- Perform an in-depth investigation of any operational anomalies, including hazardous conditions (such as water in a tank that will contain chemicals that react to water) or events. Determine why they occurred before any potentially dangerous operations are started or restarted. Provide the training necessary to do this type of investigation and create proper feedback channels to management.
- Create management of change procedures and ensure they are being followed. These procedures should include hazard analyses on all proposed changes and approval of all changes related to safety-critical operations. Create and enforce policies about disabling safety-critical equipment.
- Perform safety audits, performance assessments, and inspections using the hazard analysis results as the preconditions for operations and maintenance. Collect data to ensure safety policies and procedures are being followed and that education and training about safety is effective. Establish feedback channels for leading indicators of increasing risk.
- Use the hazard analysis and documentation created during development and passed to operations to identify leading indicators of migration toward states of higher risk. Establish feedback channels to detect the leading indicators and respond appropriately.
- Establish communication channels from operations to development to pass back information about operational experience.
- Perform in-depth incident and accident investigations, including all systemic factors. Assign responsibility for implementing all recommendations. Follow up to determine whether recommendations were fully implemented and effective.
- Perform independent checks of safety-critical activities to ensure they have been done properly.
- Prioritize maintenance for identified safety-critical items. Enforce maintenance schedules.
- Create and enforce policies about disabling safety-critical equipment and making changes to the physical system.
- Create and execute special procedures for the startup of operations in a previously shutdown unit or after maintenance activities.
- Investigate and reduce the frequency of spurious alarms.
- Clearly mark malfunctioning alarms and gauges. In general, establish procedures for communicating information about all current malfunctioning equipment to operators and ensure they are being followed. Eliminate all barriers to reporting malfunctioning equipment.
- Define and communicate safe operating limits for all safety-critical equipment and alarm procedures. Ensure that operators are aware of these limits. Assure that operators are rewarded for working within the limits and following emergency procedures, even when it turns out no emergency existed. Provide for tuning the operating limits and alarm procedures over time as required.
- Ensure that spare safety-critical items are in stock or can be acquired quickly.

## 운영(Operations)

- 운영 안전 관리 계획(operations safety management plan)을 수립한다.
- 운영자와 운영 관리자를 위한 특별 훈련을 개발하여 필요한 기술을 확보하고, 이벤트가 발생하거나 경험을 통해 더 많은 것을 배우게 될 때마다 이를 업데이트한다. 훈련에 대한 피드백, 평가 및 개선 프로세스를 만든다. 직원들이 직무를 안전하게 수행할 수 있고 안전 장비의 올바른 사용법을 이해할 수 있으며 비상 시 적절하게 대응할 수 있도록 훈련시킨다.
- 워킹 그룹을 만든다.
- 경험이 축적됨에 따라 운영 과정에서의 위험 일지와 위험 분석 결과를 유지관리하고 활용한다.
- 위험한 작업 시 모든 비상 장비(emergency equipment)와 안전 장치가 항상 작동할 수 있도록 한다. 안전 필수적, 비일상적, 잠재적으로 위험한 작업을 시작하기 전에 알람 테스트를 포함하여 모든 안전 장비가 작동하는지를 검사한다.
- 위험한 조건(예: 물에 반응하는 화학 물질이 있는 탱크 내의 물) 또는 이벤트와 같은 모든 운영 이상상황(anomalies)에 대해 심층적인 조사를 수행한다. 잠재적으로 위험한 운영이 시작되거나 재시작되기 전에 운영 이상상황이 발생한 이유를 조사한다. 이러한 유형의 조사 및 적절한 피드백 채널을 구축하여 관리에 필요한 훈련을 제공한다.
- 변경절차에 대한 관리 체계를 구축하고 지켜지도록 한다. 변경절차에는 제안된 모든 변경에 대한 위험 분석과 안전 필수 동작에 관련된 모든 변경사항의 승인이 포함되어야 한다. 안전 필수 장비 사용 제한(역주: 변경 이후에는 장비의 사용 제한이 필요할 수 있음)에 대한 정책을 만들고 이를 강제한다.
- 운영 및 유지보수의 전제 조건으로서의 위험 분석 결과를 활용하여 안전 감사, 성능 평가 및 검사(inspection)를 수행한다. 안전 정책과 절차가 준수되고 있는지, 안전에 대한 교육과 훈련이 효과적인지를 확인하기 위한 데이터를 수집한다. 증가하는 리스크에 대한 선행지표 피드백 채널을 구축한다.
- 개발 과정에서 생성되어 운영에 전달된 위험 분석 결과 및 문서를 사용하여 높은 리스크 상태로의 전환에 대한 선행지표를 식별한다. 선행지표를 탐지하고 적절하게 대응하기 위한 피드백 채널을 구축한다.
- 운영측에서 개발측으로의 피드백 채널을 구축하여 운영 경험의 정보를 역으로 전달한다.
- 사건 및 사고 조사 시 모든 시스템적 요인을 포함하여 심층적으로 조사한다. 모든 권고사항의 시행을 위해 책임을 할당한다. 권고사항이 모두 시행되었고 효과적인지를 확인하기 위한 후속조치를 수행한다.
- 안전 필수 활동에 대한 독립적인 검사(check)를 수행하여 안전 필수 활동이 적절하게 수행되었는지 확인한다.
- 식별된 안전 필수 항목에 대한 유지보수 우선순위를 지정한다. 일정에 따라 유지보수를 강제한다.
- 사용을 제한하는 안전 필수 장비 및 물리적 시스템의 변경에 대한 정책을 만들고 강제한다.
- 종료된(shutdown) Unit의 작업 시작 또는 유지보수 이후의 작업 시작을 위한 특별 절차를 만들고 실행한다.
- 가짜(spurious) 알람의 빈도를 조사하여 감소시킨다.
- 오작동(malfunctioning) 알람과 게이지를 명확히 표시한다. 일반적으로, 현재 오작동 중인 모든 장비에 대한 정보를 운영자에게 전달하는 절차를 수립하고 그 절차가 준수되는지 확인한다. 오작동 중인 장비에 대한 보고를 방해하는 모든 장애물을 제거한다.
- 모든 안전 필수 장비 및 알람 절차에 대한 안전 운영의 한계를 정의하고 전달한다. 운영자가 이러한

- Establish communication channels to plant management about all events and activities that are safety-related. Ensure management has the information and risk awareness they need to make safe decisions about operations.
- Ensure emergency equipment and response services are available and operable to treat injured workers.
- Establish communication channels to the community to provide information about hazards and necessary contingency actions and emergency response requirements.

한계를 인식하도록 한다. 비상 상황이 아니라고 판명되는 경우라도 운영자가 한계 및 비상 절차(emergency procedure)를 따르면 보상받을 수 있도록 보장한다. 추후 필요한 경우 운영 한계 및 알람 절차를 조정하도록 한다.

- 여분의 안전 필수 물품을 구비하거나 신속하게 구비될 수 있도록 한다.
- 안전 관련 모든 이벤트 및 활동에 대해 플랜트 관리자와의 의사소통 채널을 구축한다. 관리자가 운영에 대한 안전한 결정을 하는 데 필요한 정보 및 리스크를 인식하도록 한다.
- 부상당한 작업자를 치료하기 위한 비상 장비 및 대응이 가용하고 운영 가능하도록 한다.
- 커뮤니티에 의사소통 채널을 구축하여 위험, 필수적인 우발상황 조치(contingency actions), 비상 대응(emergency response) 요구사항에 대한 정보를 제공한다.

# Appendix E: Basic Engineering and Control Concepts for Non-Engineers

In reviews of an early draft of our STPA handbook, we discovered that we had assumed some engineering background that not all readers had: Users of STPA and CAST are not necessarily trained in engineering. This appendix provides an introduction to basic engineering concepts that may be unfamiliar to some users of this handbook.

I have attempted to write the sections in this appendix to be independent so that readers can pick and choose sections that interest them. No assumption is made about any particular educational background in covering these topics, which include:

- What is a "system"?
- Basic systems engineering concepts and terminology
- The concept of "control" in engineering
- Systems theory vs. complexity theory

## What is a "System"?

The most basic concept underlying everything else in this handbook is that of a *system*.

> *System*: A set of things (referred to as system components) that act together as a whole to achieve some common goal, objective, or end.

Some definitions of a system leave out the "goal" or "objective" and state essentially that a system is a connected set of things or parts forming a unified whole. This definition does not capture the way the term "system" is usually used. A shoe, a star, and a locomotive are a set of things or potential parts of a system, but most people would not normally consider this to be a system. It could be considered as a system if a purpose could be conceived for considering these individual things together; the purpose is basic to the concept.

Other definitions state that the components of the system must be interdependent or connected or interacting, but none of these conditions are really necessary to have a system. They also constrain the definition in a way that excludes things that usually are considered to be systems. The system components may be either directly or indirectly connected to each other, with the latter including connections involving the system purpose only and various types of indirect interdependencies.

The consequence of this definition is that a goal or objective for the system is fundamental. But there may be different objectives for those defining and viewing systems. An airport is used throughout this section to illustrate various points. To a traveler, the purpose of an airport may be to provide air transportation to other locales. To local or state government, an airport may be a means to increase government revenue and economic activity in the area of the airport. To the airlines, the purpose of an airport may be to take on and discharge passengers and cargo. To the businesses at the airport, the purpose is to attract customers to whom they can sell products and services. Therefore, when talking about a system, it is always necessary to specify the purpose of the system that is being considered.

*A system is an abstraction, that is, a model conceived by the viewer.*

The observer may see a different system purpose than the designer or focus on different relevant properties. Specifications, which include the purpose of the system, are critical in system engineering. They ensure consistency of mental models among those designing, using, or viewing a system, and they enhance communication. Notice that different components of the airport may be included in a

# 부록 E : 비엔지니어를 위한 기본적인 엔지니어링 및 컨트롤 개념

STPA 핸드북의 초안을 검토하면서, 전제한 일부 엔지니어링 배경지식을 모든 독자가 가진 것은 아니라는 것을 알게 되었다: STPA와 CAST의 사용자가 반드시 엔지니어링 교육을 받아야 하는 것은 아니다. 이 부록에서는 일부 사용자에게는 익숙하지 않을 수도 있는 기본적인 엔지니어링 개념에 대해 소개한다.

독자가 관심 있어 하는 섹션을 선택할 수 있도록 이 부록의 섹션을 독립적으로 작성했다. 다음과 같은 주제를 다루는 데 있어서 특정 교육 배경에 대해서는 어떠한 가정도 하지 않는다:

- "시스템"이란 무엇인가?
- 기본 시스템 엔지니어링 개념 및 용어
- 엔지니어링에서의 "컨트롤"의 개념
- 시스템 이론 vs. 복잡도 이론

## "시스템"이란 무엇인가?

이 핸드북에서 다루는 모든 것의 기반이 되는 기본 개념은 *시스템*의 개념이다.

> *시스템*: 공통된 목표, 목적 또는 결과를 달성하기 위해 전체로써 함께 동작하는 일련의 요소(시스템 컴포넌트라고 함) 집합

일부 시스템 정의에서는 "목표" 또는 "목적"을 생략한 채, 통합된 전체를 형성하는 연결된 일련의 사물 또는 부품이라고 시스템을 정의하기도 한다. 이러한 정의는 "시스템"이라는 용어가 일반적으로 사용되는 의미를 뜻하지 않는다. 신발 한 짝, 별, 기관차는 시스템의 일부 또는 잠재적 부분이지만 대부분의 사람들은 이를 시스템으로 생각하지 않는다. 이러한 개별적 사물들을 모두 함께 고려하기 위한 목적이 있다면 이는 시스템으로 간주할 수 있다; 목적은 시스템의 기본 개념이다.

다른 정의에서는 시스템의 컴포넌트가 상호 의존적이거나, 연결되거나, 상호작용해야 한다고 명시하지만 이 중 어느 것도 시스템이 필수적으로 갖추어야 하는 것은 아니다. 일반적으로 시스템이라고 여겨지는 것을 제외하는 방식으로 시스템 정의를 제한할 필요는 없다. 시스템 컴포넌트는 직접 또는 간접적으로 서로 연결될 수 있는데 후자는 시스템 목적만으로 연결된 경우나 다양한 유형의 간접 상호의존성과 관련하여 연결된 경우를 포함한다.

시스템의 정의에서 중요한 것은 시스템의 목표나 목적이 필수적(fundamental)이라는 것이다. 그러나 시스템의 목적은 그 시스템을 정의하거나 바라보는 사람에 따라 다를 수 있다. 이 섹션에서는 공항을 예제로 하여 다양한 포인트를 설명한다. 여행자에게 있어 공항의 목적은 다른 지역으로 항공 교통편을 제공하는 것이다. 지방 정부 또는 주 정부에 있어 공항은 공항 지역의 정부 수입과 경제 활동을 증대시키는 수단일 것이다. 항공사에게 공항의 목적은 승객과 화물을 인계하는 것이다. 비즈니스 측면에서의 공항의 목적은 제품과 서비스를 판매할 수 있는 고객을 확보하는 것이다. 그러므로 시스템에 대해 말할 때에는 항상 고려하는 시스템의 목적을 명시해야 한다.

> *시스템은 추상적인 것, 즉, 관찰자(viewer)가 생각하는 모델이다.*

관찰자는 시스템의 목적을 설계자와는 다르게 보거나 관련된 다른 속성에 초점을 둘 수 있다. 시스템

particular “airport” system, such as passenger check-in counters, ramps to the planes, and taxiways in the airline view of an airport versus shops and customers from the commercial view. Note again that these are models or abstractions laid upon the actual physical world by human minds, i.e., a system lies in the eye of the beholder. The components that are considered in any “airport system” or subsystem and the role they play in the system as a whole may be different for each concept (model) of an airport system or of airport subsystems. The basic idea here is that the purpose or goals of the system being considered must be specified and agreed upon by those modeling and analyzing a particular system and that these aspects of systems are abstractions or models imposed by the viewer on the real-world objects.

For engineered (man-made) systems, the purpose is usually specified before creating the system although observers of the system may interpret the purpose differently than originally intended by the designers. For natural systems, behavior may be interpreted as purposeful by the observers of the system.

There are some basic assumptions underlying the concept of a system:

- The system goals can be defined
- Systems are atomistic, that is, they can be separated into components with interactive relationships between the components regardless of whether the interactions are direct or indirect.

Systems themselves may be part of a larger system or be divisible into subsystems (viewed as components of the overall system). Note that the definition here is what is called “recursive” in mathematics and computer science. That is, the definition is made in terms of itself. A system is usually part of a larger system and it can be divisible into subsystems. Figure E.1 shows a typical abstraction hierarchy for a system labeled A (for example the system “airport”) and for three subsystems, which in turn can be conceived as systems themselves.

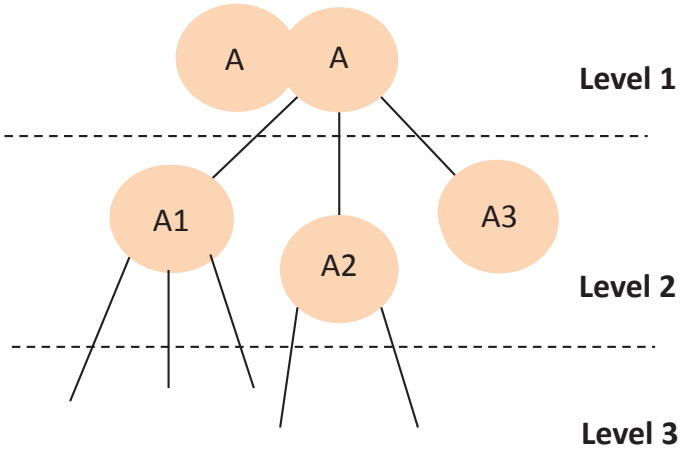



**Figure E.1**: The abstraction System A may be viewed as composed of three subsystems. Each subsystem is itself a system.

Figure E.1 is not a connection diagram. Rather it is a hierarchical abstraction that shows the different views of a system at different levels of abstraction or modeling. Level 1 conceives of the system as a whole. Level 2 visualizes it as being composed of three subsystems. Figure E.2 shows an abstraction where A itself is conceived as part of a larger system AB.

의 목적을 포함하는 명세(specification)는 시스템 엔지니어링에서 매우 중요하다. 그것은 시스템을 설계, 사용 또는 관찰하는 사람들 사이에서 멘탈 모델의 일관성을 보장하고 커뮤니케이션을 향상시킨다. 특정 "공항" 시스템에는 공항의 다른 컴포넌트가 포함될 수 있다. 예를 들어 공항 관점에서 볼 때는 승객 체크인 카운터, 비행기로의 램프(ramp), 항공사 유도로가 포함될 수 있고 상업적 관점에서 볼 때는 상점과 고객이 포함될 수 있다. 이러한 것들은 실제 물리적 세계를 대상으로 사람의 마음이 만들어낸 모델 또는 추상이다. 즉, 시스템은 바라보는 사람의 관점에 달려있다. 어떤 "공항 시스템" 또는 공항 서브시스템에서 고려되는 컴포넌트들과, 시스템 전체에서 그 컴포넌트들이 수행하는 역할은 공항 시스템 또는 공항 서브시스템의 각 개념(모델)에 따라 다를 수 있다. 여기서의 기본적인 아이디어는 고려하고자 하는 시스템의 목적이나 목표가 시스템을 모델링하고 분석하는 사람들 간 명세되고 동의되어야 한다는 것이며 시스템의 이러한 측면은 실제 세계의 오브젝트에 대해 사람들이 보는 추상화나 모델인 것이다.

엔지니어드(사람이 만든) 시스템의 경우, 일반적으로 시스템을 만들기 전에 목적을 명세하는 데 시스템을 바라보는 사람이 원래 설계자의 의도와는 다르게 목적을 해석할 수도 있다. 자연의 시스템의 경우에는 시스템을 바라보는 사람이 시스템의 동작을 의도대로 해석할 수 있다.

시스템 개념의 기본 가정은 다음과 같다:

- 시스템 목표를 정의할 수 있다.
- 시스템은 원자성을 가진다(atomistic). 즉, 시스템은 상호작용이 직접적이든 간접적이든 관계없이 컴포넌트 간 상호작용하는 관계를 갖는 컴포넌트로 나누어 질 수 있다.

시스템은 더 큰 시스템의 부분이거나 서브시스템(전체 시스템의 컴포넌트로 간주되는)으로 나뉠 수 있다. 이 정의는 수학이나 컴퓨터 과학에서 "재귀적(recursive)"이라고 불리는 것이다. 즉, 시스템의 정의는 시스템 자체로 이루어진다. 시스템은 일반적으로 더 큰 시스템의 부분이며 서브시스템으로 나뉠 수 있다. 그림 E.1은 A라는 시스템(예: "공항" 시스템)의 세 가지 서브시스템에 대한 전형적인 추상화 계층 구조를 나타내며, 서브시스템들은 그 자체로 시스템으로 볼 수 있다.

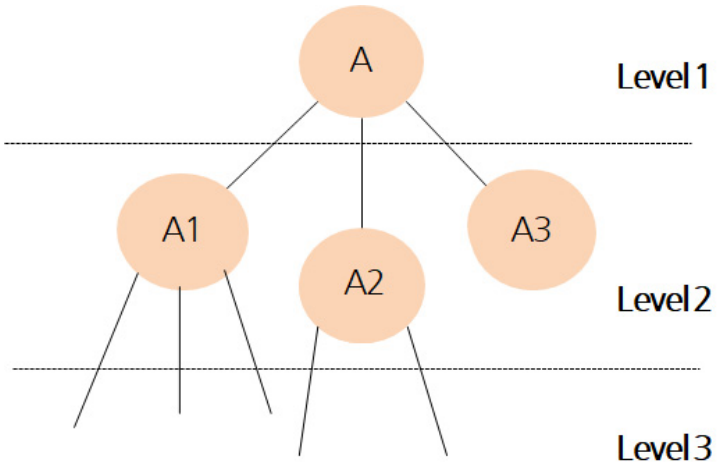



그림 E.1: 세 개의 서브시스템으로 구성된 추상화 시스템 A. 각 서브시스템 자체가 하나의 시스템임

그림 E.1은 연결을 나타낸 다이어그램(connection diagram)이 아니며 계층적 추상화를 나타낸 것으로 추상화 또는 모델링의 각 수준에서 시스템의 여러 관점을 보여준다. 레벨 1은 시스템 전체를 나타낸다. 레벨 2는 3개의 서브시스템으로 구성되어 있는 것으로 시각화한다. 그림 E.2는 A 자체가 더

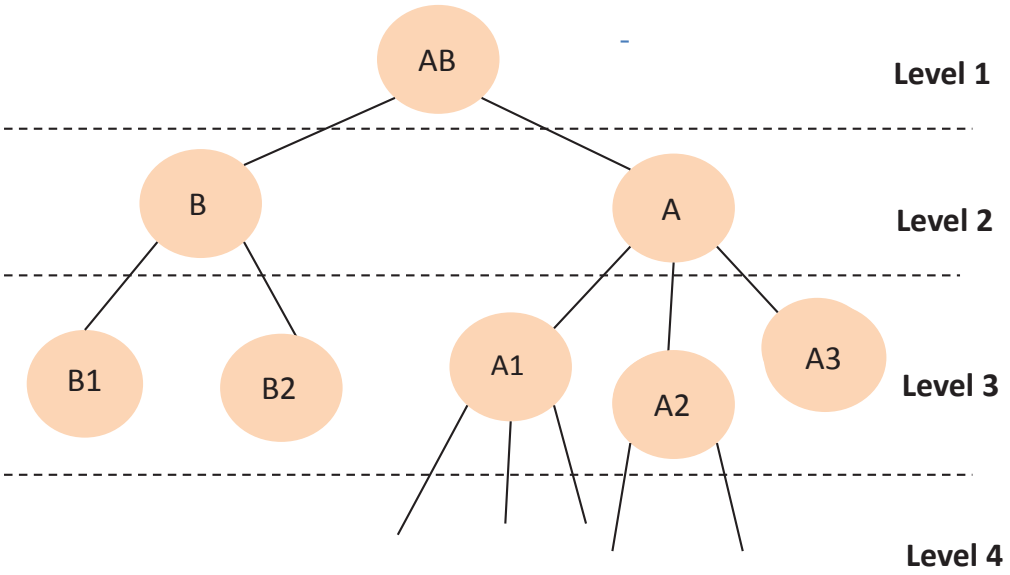
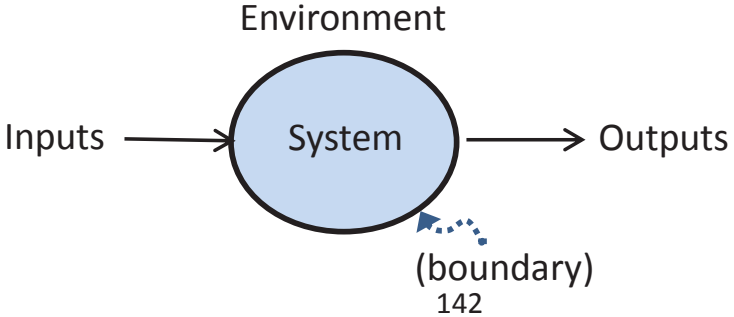



**Figure E.2**: System A can be viewed as a component (subsystem) of a larger system AB

The recursive nature of the definition of a system is important because many people have suggested that "systems of systems" must be treated differently than systems. In fact, the same general system engineering and analysis methods and techniques are applicable to all systems. A "system of systems" is just a "system" when using the definition of a system as defined in system theory and as the concept is used in engineering. When one puts together several systems, you get not a system of systems but an entirely new and unique system. It is not a summation of several systems.

Systems have *states*. A state is a set of relevant properties describing the system at any time. Some properties of the state of an airport viewed as an air transportation system may be the number of passengers at a particular gate, where the aircraft are located and what they are doing (loading passengers, taxiing, taking off, or landing). The components of the state that are relevant depend on how the boundaries are drawn between the system and its environment.

The *environment* is usually defined as the set of components (and their properties) that are not part of the system but whose behavior can affect the system state. Therefore, the system has a state at a particular time and the environment has a state. The concept of an environment implies that there is a boundary between the system and its environment. Again, this concept is an abstraction created by the viewer of the system and need not be a physical boundary. What is part of the system or part of the environment will depend on the particular system and its use at the time.



큰 시스템 AB의 일부로 인식되는 추상화를 보여준다.

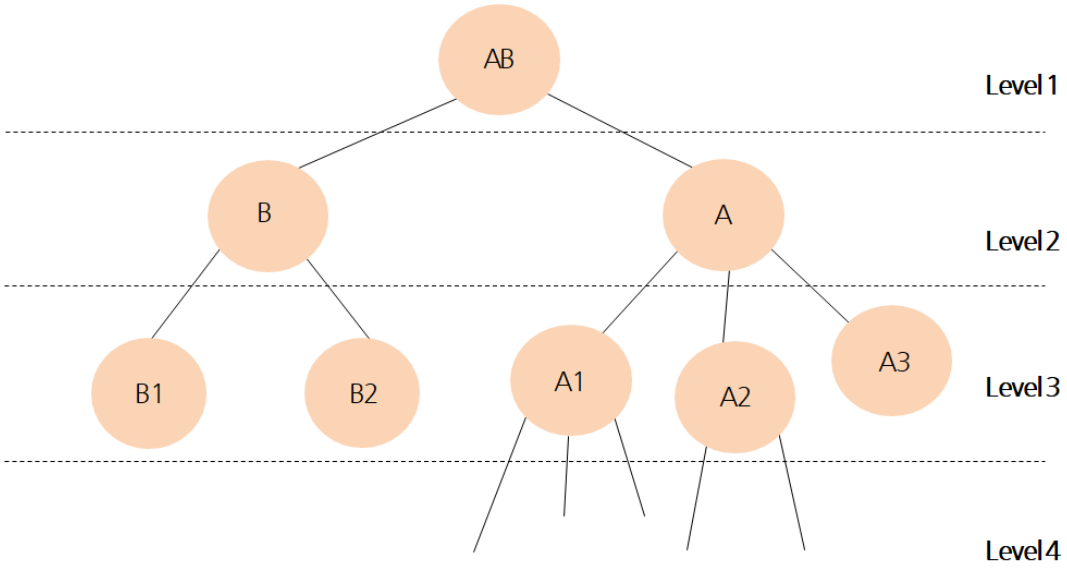
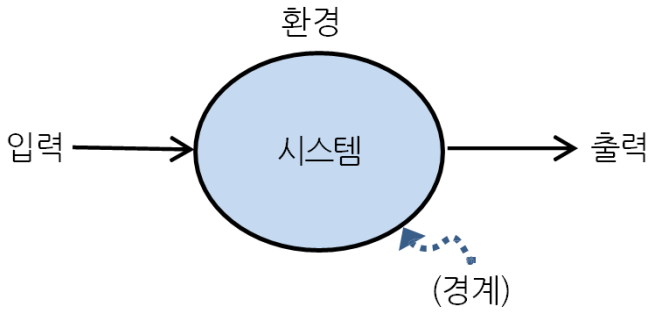



그림 E.2: 시스템 A는 더 큰 시스템 AB의 컴포넌트(서브시스템)로 볼 수 있음

많은 사람들이 시스템과 "시스템의 시스템(systems of systems)"을 다르게 취급해야 한다고 주장하기 때문에 시스템 정의 시 재귀적 성격을 언급하는 것이 중요하다. 실제로, 일반적인 시스템 엔지니어링, 분석 방법 및 기술이 모든 시스템에 동일하게 적용된다. "시스템의 시스템(system of systems)"은 시스템 이론에서의 시스템 정의를 사용할 때, 엔지니어링에서 사용되는 개념인 "시스템"일 뿐이다. 여러 시스템을 하나로 모으면 시스템의 시스템이 아니라 완전히 새롭고 독특한 시스템을 얻을 수 있다. 그 시스템은 여러 시스템의 합이 아니다.

시스템에는 *상태(state)*가 있다. 상태는 모든 시점에서의 시스템을 설명하는 관련 속성(properties)의 집합이다. 항공 운송시스템 관점에서 공항의 상태 중 일부 속성은 특정 게이트의 승객 수, 항공기가 위치한 곳, 그리고 무엇을 하는지(승객 탑승, 유도, 이륙, 또는 착륙)와 같은 것일 수 있다. 관련된 상태의 컴포넌트는 시스템과 환경간의 경계가 그려지는 방식에 따라 다르다.

*환경(environment)*은 일반적으로 시스템의 일부가 아닌 컴포넌트(및 그것들의 속성)의 집합으로 정의되지만, 그것들의 행위는 시스템의 상태에 영향을 줄 수 있다. 따라서 시스템은 특정 시간에서의 상태를 가지고 환경은 (시간과 무관하게) 상태를 가진다. 환경의 개념은 시스템과 환경 사이에 경계가 있음을 의미한다. 다시 말하지만, 이 개념은 시스템 관찰자에 의해 만들어진 추상적인 것이며 물리적 경계일 필요는 없다. 시스템의 일부 또는 환경의 일부가 무엇인지는 특정 시스템과 그 당시의 용도에 따라 달라진다.



System *inputs* and *outputs* cross the system boundary. This concept is usually called an *open* system. There is also a concept of a *closed system* (which has no inputs or outputs), but it does not have much relevance for the engineered systems with which we are most concerned in system safety.

## The Concept of "Control" in Engineering

The concept of control is important in the conception, design, and operation of a system. A system can conceivably operate without any type of control over its behavior, but it would be difficult to ensure that the system satisfied its goals while at the same time constraining the way it achieves those goals so that adverse, unwanted consequences do not also result.

Control is basic to engineering, especially complex systems. Engineers are dealing not with living things, but with man-made things —automobiles, dams, aircraft, chemical plants, spacecraft, washing machines, robots—that are built to accomplish some goal. If they are not inert (like a bridge), there is a need to operate or control their operation in terms of the states that they get into.

Non-engineers sometimes interpret the word "control" differently than the way it is used in engineering. Control is not about forcing individual compliance to specified roles and procedures through some type of militaristic-style authority. Rather, control is being used here in a very broad sense and may be implemented through design controls like interlocks and fail-safe design, through process controls such as maintenance and manufacturing procedures, or even social constructs such as culture, incentive structures, and individual self-interest. Without the imposition of some form of control, there would be no way to ensure that the system goals and constraints are achieved.

Simple design features acting as controls often can improve safety without also increasing complexity and cost, but this usually requires considering safety early in the design process. The most effective way to increase safety through design is to use a design that eliminates hazardous states. Next best is to design such that hazards are rare and easy to handle if they do occur. A design that reacts to the occurrence of hazards by minimizing the resulting damage is clearly the least desirable form of hazard control but often such controls must be included.

A control loop is thus only one form of control. I emphasized it in *Engineering a Safer World* because the other aspects of basic design for safety were covered so extensively in my previous book titled *Safeware*. In addition, system theory emphasizes the concept of the control loop or active control. It is not possible to teach the techniques used to design for safety in this appendix, but some basic concepts such as the distinction between p*assive* and *active* control may be helpful in understanding general safety design techniques.

There are three types of design techniques to "control" safety. The first is to use an intrinsically or inherently safe design. An intrinsically safe design is one that is not capable of producing the hazard of concern. For example, the system design may not have sufficient energy to cause an explosion. If the concern is with the use of potential toxic substances, there may be non-toxic substitutes. If the potential exists for lost information over a communication network, then more direct communication may be used if it is feasible.

If an intrinsically safe design is not possible, the use of passive control mechanisms may be possible. Passive controls do not require a positive action in order to be effective, but instead rely on basic physical principles, such as gravity. A physical interlock that prevents the system from entering a hazardous state without any overt control action is a passive control mechanism. Examples include:

시스템 *입력(input)*과 *출력(output)*은 시스템 경계를 가로지른다. 이 개념을 일반적으로 *개방형 시스템(open system)*이라고 부른다. 입력 또는 출력이 없는 *폐쇄형 시스템(closed system)*이라는 개념도 있지만 시스템 안전에서 우리가 가장 관심을 갖는 엔지니어드 시스템과는 별로 관련이 없다.

## 엔지니어링에서 "컨트롤"의 개념

컨트롤의 개념은 시스템의 개념, 설계, 운영에 있어 중요하다. 시스템의 동작에 대한 어떤 유형의 컨트롤 없이도 시스템이 운영될 수 있을 것 같지만, 시스템이 목표를 달성하는 것과 동시에 그 목표를 달성하기 위한 방법을 제한하여 원하지 않는 부정적인 결과가 발생하지 않도록 하는 것은 어렵다.

컨트롤은 엔지니어링의 기본이며 복잡한 시스템에서는 특히 그렇다. 엔지니어는 살아있는 것이 아니라 사람이 만든 것을 다룬다. 예를 들면, 어떤 목표를 달성하기 위해 만들어진 자동차, 댐, 항공기, 화학 플랜트, 우주선, 세탁기, 로봇 등이다. (다리(bridge)와 같이) 자력으로 움직이는 것이 아닌 경우, 그것들이 놓인 상태의 관점에서 그것들을 운영하거나 운영을 컨트롤해야 한다.

엔지니어가 아닌 사람들은 "컨트롤"이라는 단어를 엔지니어링에서 사용하는 방식과 다르게 해석하는 경우가 있다. 컨트롤은 군사적 방식(militaristic-style)의 통제권한을 통해 특정 역할과 절차를 개별적으로 준수할 것을 강요하는 것이 아니다. 컨트롤은 오히려 매우 광범위한 의미로 사용되고 있으며 인터락(interlock)과 페일세이프(fail-safe) 설계와 같은 설계 컨트롤, 유지보수 및 제조 절차와 같은 프로세스 컨트롤, 또는 문화, 인센티브 구조 및 개인 이익과 같은 사회적 구조를 통해서 구현될 수 있다. 어떤 형태든 컨트롤을 도입하지 않으면 시스템 목표와 제약사항을 만족시킬 수 있는 방법은 없다.

컨트롤로써 동작하는 간단한 설계의 특징은 종종 복잡도와 비용을 증가시키지 않으면서도 안전을 향상시킬 수 있다는 것이다. 그러나 일반적으로 설계 초기에 안전을 고려해야 한다. 설계를 통해 안전을 향상시키는 가장 효과적인 방법은 위험한 상태를 제거하는 설계를 하는 것이다. 차선책으로는, 위험이 발생하는 경우 그 위험이 매우 드물게 발생하고 다루기 쉽도록 설계하는 것이다. 발생하는 피해를 최소화하는 방식으로 위험 발생에 대응하는 설계는 그다지 바람직하지 않은 위험 컨트롤 방식이지만 종종 그러한 컨트롤이 포함되어야 한다.

따라서 컨트롤 루프는 컨트롤의 한 가지 형식이다. 안전을 위한 기본 설계의 다른 측면들은 *Safeware*라는 책에서 광범위하게 다루어졌기 때문에 *Engineering a Safer World*에서는 컨트롤 루프를 강조하였다. 또한 시스템 이론은 컨트롤 루프 또는 능동 제어(active control)의 개념을 강조한다. 이 부록에서 안전을 설계할 때 사용하는 기법을 가르칠 수는 없지만 *수동(passive)* 및 *능동(active)* 제어의 구분과 같은 일부 기본 개념은 일반적인 안전 설계 기술을 이해하는 데 도움이 될 수 있다.

안전을 "컨트롤"하는 세 가지 유형의 설계 기법이 있다. 첫 번째는 본질적으로 또는 선천적으로 안전한 설계를 하는 것이다. 본질적으로 안전한 설계는 우려되는 위험이 발생할 수 없는 설계를 말한다. 예를 들어, 폭발을 일으킬 만큼 충분한 에너지를 갖지 않도록 시스템을 설계할 수 있다. 잠재적 독성 물질 사용의 우려가 있는 경우 독성이 없는 대체 물질을 사용할 수 있다. 통신 네트워크를 통해 정보 손실 가능성이 있는 경우 가능하면 직접 통신을 사용할 수 있다.

본질적으로 안전한 설계가 불가능한 경우 수동 제어 메커니즘을 사용할 수 있다. 수동 제어는 효과적이기 위해 적극적(positive) 조치가 필요하지 않고 대신 중력과 같은 기본적인 물리적 원리를 이용한다. 어떤 명시적인 컨트롤 액션 없이 시스템이 위험한 상태로 들어가는 것을 방지하는 물리적 인터락은 수동 제어 메커니즘이다. 다음과 같은 예시가 있다.

- A pressure sensitive mat or light curtain that shuts off power to a robot or dangerous machinery if someone comes near.
- A physical device that ensures the correct sequencing of valve turn-off and turn-on or ensures that two valves cannot both be on or off at the same time.
- A freeze plug in a car's engine cooling system where expansion will force the plug out rather than crack the cylinder if water in the block freezes.
- A fusible plug in a boiler that becomes exposed if there is excessive heat and the water drops below a predetermined level. In that event, the plug melts and the opening allows the steam to escape, which reduces the pressure in the boiler and prevents an explosion.
- A speed governor that does not allow speeds over a specific limit or relief valves that maintain pressure below dangerous levels.

Passive controls are often designed so that the system essentially fails into a safe state. In fact, the basic approach to aircraft safety is to build the system to be fail safe. Some examples of fail-safe design are:

- Old railway semaphores that used weights to ensure that if the cable (controlling the semaphore) broke, the arm would automatically drop into the STOP position.
- Air brakes that are held in an off position by air pressure. If the brake line breaks, air pressure is lost and the brakes are automatically applied.
- A deadman switch where the operator applies continual pressure. If something happens to the operator and the pressure is not applied, the system fails into a safe state.
- A bathyscope where ballast is held in place by magnets. If electrical power is lost, the ballast is released and the bathyscope ascends to the surface.
- Designs where the effects of a failure (such as fan blades being ejected when an aircraft engine fails) are contained so that adjacent components are not affected.

An *active control*, in contrast, requires a hazardous condition to be detected and corrected. Active controls today often involve the use of computers and the basic control loops described and used throughout this handbook. Notice that there is more that can go wrong with active controls, e.g., the failure or hazardous state may not be detected or it may be detected but not corrected or it may not be corrected in time to prevent a loss. Passive controls are more reliable as they usually depend on physical principles and simpler designs while active control depend on less reliable detection and recovery mechanisms and usually much more complex designs. Passive controls, however, tend to be more restrictive in terms of design freedom and are not always feasible to implement in complex systems.

Active controls usually involve a control loop.

## What is a Control Loop?

A control system commands, directs, or regulates the behavior of other devices or processes using control loops. Such control systems may range from a single home heating controller using a thermostat to control a boiler to large industrial control systems used for controlling complex processes and machinery.

A very basic control loop is shown below (and elsewhere in this handbook):

- 누군가가 가까이 오면 로봇이나 위험한 기계의 전원을 차단하는 압력 감지 매트 또는 라이트 커튼
- 밸브를 끄고 켜는 올바른 순서를 보장하거나, 두 밸브를 동시에 켜거나 끌 수 없게 하는 물리적 장치
- 블록의 물이 얼어붙은 경우 실린더를 깨뜨리지 않고 팽창시켜 플러그를 강제로 끄는 자동차 엔진 냉각 시스템의 동결 플러그
- 과열이 발생하고 물이 사전에 설정한 수준 이하로 떨어지면 노출되는 보일러의 용해 플러그. 이 경우, 플러그가 녹고 입구에서 증기가 빠져 나와 보일러의 압력을 감소시키고 폭발을 방지함
- 특정 제한 속도 이상을 허용하지 않는 속도 조절기 또는 위험한 수준 이하의 압력을 유지하는 완화 밸브

수동 제어는 시스템이 기본적으로 안전한 상태로 실패하도록 설계되는 경우가 많다. 실제로 항공기 안전의 기본 접근법은 시스템을 페일세이프(fail-safe)하게 만드는 것이다. 페일세이프 설계의 예시는 다음과 같다.

- 수기 신호(semaphore)를 제어하는 케이블이 끊어지면 차단기가 자동으로 STOP 위치로 떨어지게 하기 위해 무게 추를 사용하는 옛날의 철도 수기 신호
- 공기 압력에 의해 오프(off) 위치에 고정되는 에어브레이크. 브레이크 라인이 끊어지면 공기 압력이 손실되고 브레이크가 자동으로 적용됨
- 운영자가 지속적인 압력을 가하는 데드맨 스위치(deadman switch). 운영자에게 무슨 일이 발생하여 압력이 가해지지 않으면 시스템은 안전한 상태로 실패함
- 밸러스트(ballast)가 자석에 의해 유지되는 심해 관측경. 전력이 손실되면 밸러스트가 해제되고 심해 관측경은 수면으로 올라감
- 설계 시 실패의 영향을 고려하여(예를 들어, 항공기 엔진 고장 시 팬 날개가 튀어 나옴), 실패로 인해 인접한 컴포넌트가 영향 받지 않음

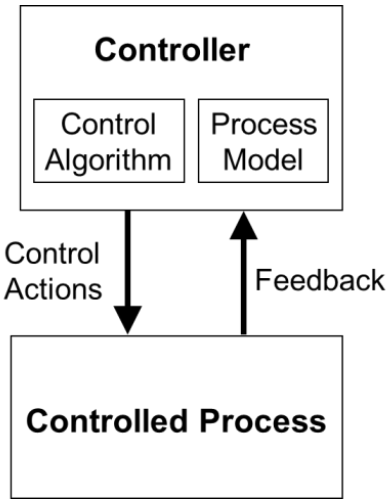
반대로 *능동 제어(active control)*는 위험 조건의 탐지 및 교정이 필요하다. 오늘날 능동 제어는 이 핸드북의 전반에 걸쳐 기술되고 사용되는 기본 컨트롤 루프를 종종 사용한다. 실패 및 위험한 상태가 탐지되지 않거나 탐지되어도 수정되지 않은 경우 또는 손실 방지를 위한 수정이 제때 이루어지지 않는 경우 등 능동 제어와 관련하여 문제가 있을 수 있다는 점을 유의해야 한다. 능동 제어는 신뢰성이 떨어지는 탐지와 복구 메커니즘에 의존하고 일반적으로 훨씬 복잡한 설계를 가지는 반면, 수동 제어는 일반적으로 물리적 원리와 단순 설계에 의존하기 때문에 보다 신뢰할 수 있다. 그러나 수동 제어는 설계 자유도라는 측면에서는 보다 제한적이 경향이 있으며 복잡한 시스템에서 구현하는 것이 항상 가능하지는 않다.

능동 제어에는 일반적으로 컨트롤 루프가 수반된다.

## 컨트롤 루프란 무엇인가?

컨트롤 시스템은 컨트롤 루프를 사용하여 다른 장치나 프로세스의 동작을 명령, 지시 또는 규제한다. 이러한 컨트롤 시스템은 보일러를 제어하기 위해 온도조절장치를 사용하는 단일 가정용 난방 컨트롤러부터, 복잡한 프로세스와 기계를 제어하는 대형 산업 컨트롤 시스템까지 다양하다.

아래 그림은(그리고 이 핸드북의 다른 부분에) 매우 기본적인 컨트롤 루프를 보여준다:



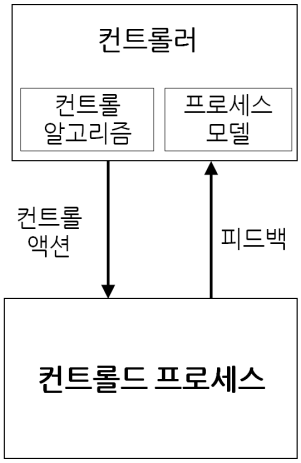

In order to control a process, the controller must have a *goal* or goals, which can include maintaining constraints on the behavior of the controlled process. In addition, the controller must have some way to affect the behavior of the controlled process, i.e., the state of the controlled process or system. These are labeled control actions in the figure. In engineering, control actions are implemented by *actuators*. In order to know what control actions are necessary, the controller must be able to determine the current state of the system. In engineering terminology, information about the state of the system is provided by *sensors* and is called *feedback*. Finally, the controller must contain some model of the state of the controlled process as explained elsewhere in the handbook.

As an example, a simple thermostat may have a goal of maintaining a temperature within a specific range. Feedback provides information to the controller about the current state of the controlled process, in this case the temperature of the air in the room. The feedback is used to update the controller's model of the process. Other information may also be part of this process model, such as environmental information (outside air temperature) or basic information about natural temperature fluctuations. The controller uses the process model to decide what control actions to provide, e.g., apply hot air or cool air, in order to change the state of the room temperature (controlled process) to stay within the required range.

There are two general operational modes for a control loop: feedback control and feedforward control. *Feedback control* is what was described in the paragraph above. When driving, a driver may read the speedometer (feedback) and decide to brake or step on the accelerator to keep the automobile's speed at a desired level.

An example of *feedforward control* occurs when the driver approaches a hill. The driver could wait until the car starts to slow down and then step on the accelerator, but more likely an experienced driver will anticipate that acceleration will be required to maintain a constant speed when going up the hill and the driver will increase acceleration before the car actually slows down. Thus, in feedforward control, the controller uses a model of the current state of the process (in this case the car speed) and the future (operating on an incline) and then provides a control action without specific feedback to identify the need.

Often feedback and feedforward control are used in tandem. In our example, the driver might anticipate the need to step on the accelerator before feedback is received using feedforward control, but feedback can be used to adjust the feedforward control actions so that a constant speed is maintained on the incline if the feedforward calculations are not perfect.




컨트롤러는 프로세스를 컨트롤하기 위해 하나 이상의 *목표(goal)*를 반드시 가져야하며 컨트롤드 프로세스의 동작에 제약사항을 유지해야(maintaining constraints) 한다. 또한 컨트롤러에는 컨트롤드 프로세스의 동작에 영향을 주기 위한 방법이 있어야 한다. 즉, 컨트롤드 프로세스의 동작은 컨트롤드 프로세스의 상태 또는 시스템의 상태를 말한다. 이 방법을 그림에서 컨트롤 액션으로 표기하였다. 엔지니어링에서 컨트롤 액션은 *액추에이터(actuators)*에 의해 구현된다. 컨트롤러는 어떤 컨트롤 액션이 필요한지 알기 위해 시스템의 현재 상태를 결정할 수 있어야 한다. 공학 용어에서 시스템 상태 정보는 *센서(sensors)*가 제공하며 이것을 *피드백(feedback)*이라고 부른다. 마지막으로, 핸드북의 다른 부분에서 설명된 바와 같이 컨트롤러에는 컨트롤드 프로세스 상태에 대한 모델(model of the state of the controlled process)이 포함되어야 한다.

예를 들어 간단한 온도조절장치는 온도를 특정 범위로 유지하는 목표를 가질 수 있다. 피드백은 컨트롤러에게 컨트롤드 프로세스의 현재 상태 정보를 제공하는데 이 경우에는 방의 온도를 제공한다. 피드백은 컨트롤러의 프로세스 모델을 업데이트 하는 데 사용된다. 환경 정보(외부 기온)나 자연적인 온도 변동에 대한 기본적인 정보와 같은 다른 정보들도 해당 프로세스 모델의 일부가 될 수 있다. 컨트롤러는 어떤 컨트롤 액션을 제공할지를 결정하는 데 프로세스 모델을 사용한다. 예를 들면 방의 온도가 요구 범위 내에서 유지될 수 있도록 방 온도를 변경하기 위한(컨트롤드 프로세스) 열풍 또는 냉풍을 작동한다.

컨트롤 루프에는 피드백(feedback) 컨트롤과 피드포워드(feedforward) 컨트롤이라는 두 가지 일반적인 운영 모드가 있다. *피드백 컨트롤(feedback control)*은 위 단락에서 설명한 것이다. 운전할 때 운전자는 속도계(피드백)를 읽고 자동차의 속도를 원하는 수준으로 유지하기 위해 브레이크를 밟을지 액셀러레이터를 밟을지를 결정한다.

*피드포워드 컨트롤(feedforward control)*의 예로 운전자가 언덕에 접근하는 경우를 들 수 있다. 운전자가 차의 속도가 느려질 때까지 액셀러레이터를 밟는 것을 기다릴 수도 있지만 숙련된 운전자는 언덕을 올라갈 때 일정한 속도가 유지되기 위해서는 가속이 필요함을 예상하고 차가 실제로 느려지기 전에 가속도를 높일 가능성이 높다. 이와 같이 피드포워드 컨트롤에서 컨트롤러는 프로세스의 현재 상태(이 경우, 차의 속도)와 미래(경사면에서 동작)의 모델을 사용하여 컨트롤의 필요 여부를 식별하는, 특정한 피드백 없이도 컨트롤 액션을 제공한다.

종종 피드백과 피드포워드 컨트롤은 동시에 사용된다. 이 예시에서, 운전자는 피드포워드 컨트롤을 사용하여 피드백을 받기 전에 액셀러레이터를 밟아야 한다고 예측할 수도 있지만 피드포워드 계산이 완벽하지 않은 경우에는 경사에서 일정한 속도가 유지되도록 피드백을 사용하여 피드포워드 컨트롤 액션을 조정할 수 있다.

The engineering concept of control (which is based on system theory) can also be applied to social and organizational systems and has been used extensively in management theory and social sciences.

## What is Systems Engineering?

System engineering is the attempt to put structure into the design and construction of a system in order to improve the results of the engineering effort. For relatively simple systems, system engineering may not be necessary. Systems engineering came into being after World War II when we started building significantly more complex systems, especially missile and other defense systems, and found that an informal design and construction process often resulted in systems that did not satisfy the goals envisioned for the system and the constraints on its potential behavior, i.e., constraints how it achieved the goals. Lack of a structured process also led to projects being late and over budget.

System engineering is a large subject, but only two concepts are necessary to understand this handbook. The first is the concept of the system engineering phases and process. The most basic model of these phases is shown in Figure E.3.

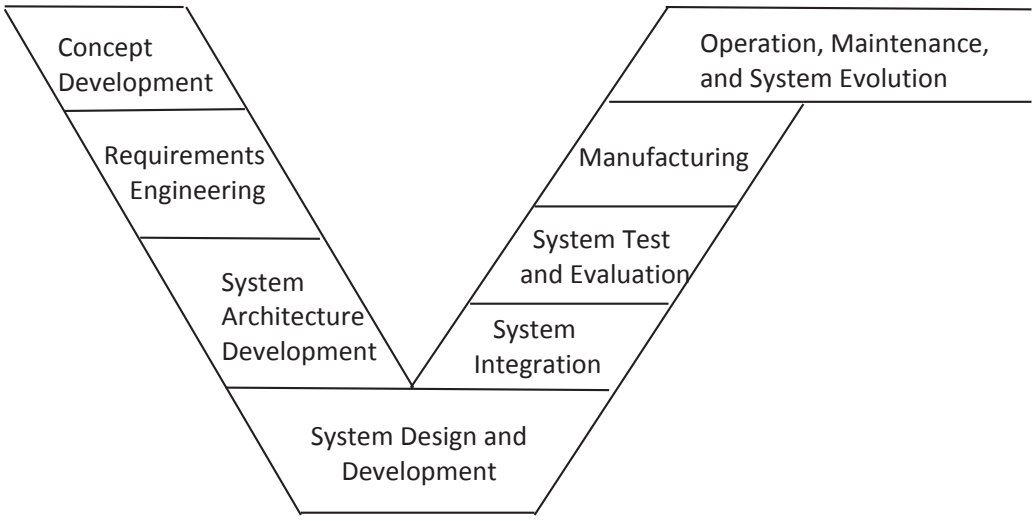



**Figure E.3**: The basic system engineering "V" model

This model is called the V-model, although different labels may be placed on the various components. Sometimes the phases are drawn in a straight line (if the line tilts downward it is called the "waterfall" model), but there is no difference except in the way it is drawn. The basic idea is that the best results ensue if a structured process is used, where the system concepts are first developed and the basic goals and constraints on the system are defined. There may be various feasibility and other analyses done at this early time in development to stop the process from going down paths that require retracing later. Requirements engineering is usually the next step in the process where detailed requirements are developed for the system given the basic goals and constraints earlier agreed upon. System architecture development means that a basic architecture or high-level design of the system is created before detailed design and development. The left side of the "V" represents the basic design process.

The right side of the V shows the later stages in development when assurance and manufacturing take place. Sometimes operation of the system is included (which is then called a life-cycle model)—as

컨트롤의 엔지니어링 개념(시스템 이론에 기반한)은 사회, 조직 시스템에도 적용될 수 있으며 경영 이론 및 사회 과학 분야에서 광범위하게 사용되어 왔다.

## 시스템 엔지니어링이란 무엇인가?

시스템 엔지니어링은 엔지니어링 활동의 결과를 향상시키기 위해 시스템의 설계 및 구축 프로세스를 구조화하는 것이다. 상대적으로 간단한 시스템의 경우 시스템 엔지니어링이 필요하지 않을 수도 있다. 시스템 엔지니어링은 제2차 세계 대전 이후 미사일 및 기타 방어 시스템과 같은 매우 복잡한 시스템을 구축하기 시작했을 때 생성되었다. 비정형(informal) 설계 및 구축 프로세스로 인해 종종 시스템의 계획된 목표를 충족시키지 못하였고 시스템의 잠재적 동작에 대한 제약사항, 즉, 어떻게 목표를 달성할 것인지에 대한 제약사항을 충족시키지 못하였다. 또한 구조화된 프로세스의 부족으로 인해 프로젝트가 지연되고 예산이 초과되었다.

시스템 엔지니어링은 커다란 주제이지만 이 핸드북을 이해하기 위해서는 두 가지 개념만 필요하다. 첫 번째는 시스템 엔지니어링 단계와 프로세스의 개념이다. 이러한 단계의 가장 기본적인 모델은 그림 E.3에 나와 있다.

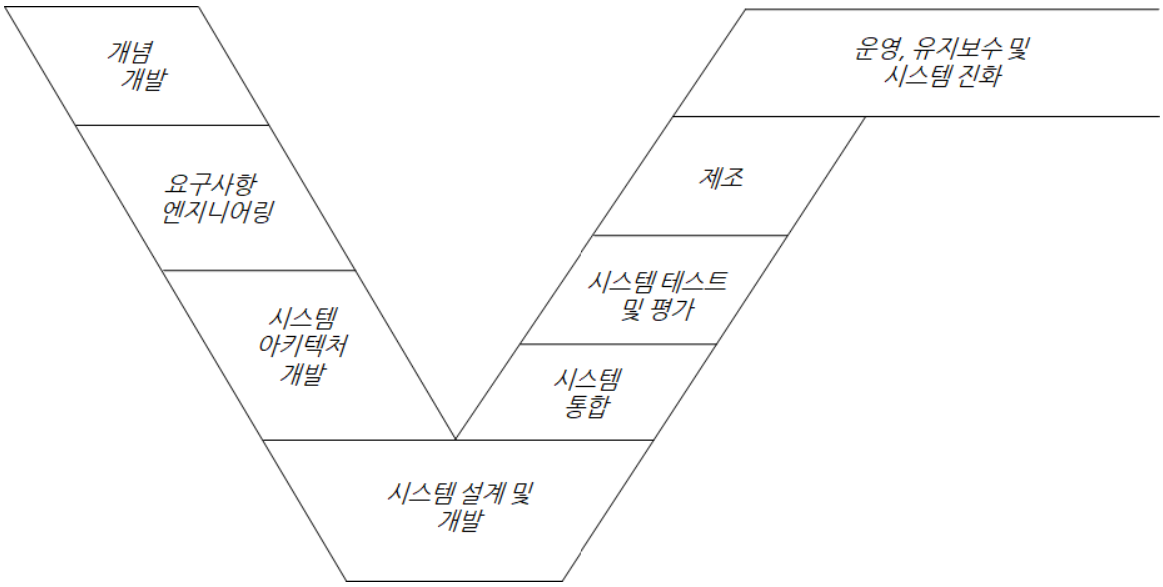



그림 E.3: 기본적인 시스템 엔지니어링 "V-모델"

이 모델을 V-모델이라 부르는데 각 단계는 다른 명칭으로 칭할 수도 있다. 때로는 각 단계가 직선으로 그려지는 경우도 있다(선이 아래쪽으로 기울면 "폭포수" 모델이라고 부름). 그러나 그려지는 방법을 제외하고는 차이가 없다. 기본 아이디어는, 시스템 개념(system concepts)을 처음에 개발하고 시스템의 기본 목표와 제약사항을 정의하는 구조화된 프로세스를 사용한다면 최상의 결과를 도출할 수 있다는 것이다. 나중에 프로세스를 되풀이하는 상황을 방지하기 위해 개발 초기 단계에 여러 타당성(feasibility) 및 다른 분석을 수행할 수 있다. 일반적으로 다음 단계는 요구공학(requirement engineering)이며, 합의된 기본 목표 및 제약사항에 기반하여 세부 요구사항을 개발한다. 시스템 아키텍처 개발(system architecture development)은 상세 설계와 개발을 수행하기 전에 시스템의 기본 아키텍처 또는 시스템의 상위 수준 설계를 하는 것을 의미한다. V-모델의 왼쪽 부분은 기본 설계 프로세스를 나타낸다.

shown in Figure F.3. On the right side of the V-model process, the various components that have been designed and constructed are integrated and go through a testing and evaluation phase. They are then manufactured and used.

The figure above is purposely simplified to reduce clutter and only reflects the overall process components. There is always lots of bouncing around the phases and not one straight-line process. Requirements are never totally specified at the beginning; the design process itself will generate more understanding of the problem being solved and therefore result in adding to or changing the original requirements and constraints. Serious problems during development may occasionally require the project to revert totally to an earlier phase. But overall, a step-wise process is generally followed.

In addition, this model should not be taken too literally. The labeling of phases does not mean that some parallelism is not possible and, in fact, common. Waiting for all testing to take place, for example, until the end creates grave risks to a project. Testing of various kinds may start in the earliest concept phase (perhaps in the form of simulations or prototyping) and usually continues through every phase. Also, various labels may be applied to the phases, depending on the type of system being designed. The goal is simply to define a structured process that will be tailored for the various needs of specific projects.

Why is all of this necessary for accident investigators and analysts to understand? While accidents occur during operations, the design flaws that led to them arise during development. The B737 MAX problems are an example of where it is not possible to simply blame the pilots (although people have tried). Accident investigations need to identify why the design flaws that led to the loss were introduced and why they were not identified before operational use of the system. Tracing the causes of accidents back to engineering and development is going to become more and more important as the complexity of the systems we are creating increases, making design flaws an important factor in accidents. To thoroughly understand why an accident occurred, we need to understand where any design flaws were introduced and why they were not identified before the system went into operational use. There are (or at least should be) many procedures designed into the development process that should find the design flaws before the system becomes operational. Investigating why such procedures were not effective is a large and important component of continual improvement in the development process.

## Systems Theory vs. Complexity Theory

STAMP is based on systems theory, not complexity theory. Contributions to systems theory have been made by many people, but Ludwig von Bertalanffy, an Austrian biologist, is credited as one of the founders of what he called general systems theory. Norbert Weiner explored the implications for mathematics and engineering. Weiner called his theory *cybernetics,* but that term has faded over time and Bertalanffy's terminology is generally used today.

Systems theory, as you have seen in this handbook and perhaps elsewhere, is a set of principles that can be used to understand the behavior of complex systems, whether they be natural or man-made systems. *Systems thinking* is the term often used to describe what people are doing when they apply systems theory principles. These principles are briefly described in Chapter 1 of this handbook.

*Complexity theory* grew out of systems theory and other concepts in the 1960s and is usually associated with the Santa Fe Institute and researchers working there. Some commonalities exist between Systems Theory and Complexity Theory in that both include terms like emergence and focus on complex system behavior as a whole rather than on reduction or decomposition into components. The basic components of system theory are emergence, hierarchy, communication, and control, and these also are included in complexity theory. Both systems theory and complexity theory also include concepts

V-모델의 오른쪽 부분은 보증과 제조(assurance and manufacturing)가 이루어지는 개발의 후반 단계를 보여준다. 그림 E.3에서와 같이 종종 시스템의 운영이 포함된다(이를 수명주기 모델이라고 함). V-모델 프로세스의 오른쪽 부분에서, 설계되고 구축된 여러 컴포넌트가 통합(integrated)되어 테스트 및 평가(testing and evaluation) 단계를 거친다. 그 후 제작되고 사용된다(manufactured and used).

위의 그림은 혼란을 줄이기 위해 의도적으로 단순화 되었으며 전체 프로세스 컴포넌트만을 반영하고 있다. 하나의 직선 프로세스가 아니라 항상 여러 단계를 거치면서 수차례 앞뒤를 오간다. 요구사항은 초기에 완전히 명세되지 않는다; 이는 설계 프로세스에서 문제 해결의 이해도가 높아짐에 따라 기존의 요구사항과 제약사항을 추가하거나 변경하기 때문이다. 개발 과정에서 심각한 문제로 인해 프로젝트가 완전히 초기 단계로 되돌아가야 할 수도 있다. 그러나 일반적으로 단계적 프로세스를 따르게 된다.

또한, 이 모델을 있는 그대로 사용해서는 안 된다. 단계를 구분하여 표시한 것이 각 단계를 병행하는 것이 불가능함을 의미하는 것은 아니며 실제로도 병행한다. 예를 들어 모든 테스트가 끝날 때까지 기다리는 것은 프로젝트에 심각한 리스크를 초래한다. 초기 개념 단계에서 (시뮬레이션 또는 프로토타입 형태로) 다양한 종류의 테스트를 시작할 수 있으며 일반적으로 모든 단계에 걸쳐 계속된다. 또한 설계 중인 시스템의 유형에 따라 다양한 라벨이 각 단계에 적용될 수 있다. 특정 프로젝트의 다양한 요구에 맞춰 구조화된 프로세스를 정의하는 것이 목표이다.

사고 조사관과 분석가들이 이러한 모든 것들을 이해해야 하는 이유는 무엇일까? 사고는 운영 중에 발생하지만 사고를 유발하는 설계상의 결함은 개발 중에 발생한다. B737 MAX 문제는 단순히 조종사를 비난할 수 없는(실제로는 비난하려 했지만) 사례이다. 사고 조사에서는 손실을 초래한 설계 결함이 도입된 이유와 시스템의 운영 전에 왜 결함이 식별되지 않았는지를 파악할 필요가 있다. 우리가 만들고 있는 시스템의 복잡성이 증가함에 따라 엔지니어링과 개발 과정에서 사고의 원인을 추적하는 것이 점점 더 중요해질 것이고 설계 결함이 사고의 중요한 요인이 되고 있다. 사고가 발생한 이유를 철저하게 파악하려면 설계 결함이 어디서 도입되었고 시스템을 운영하기 전에 식별되지 않은 이유를 알아야 한다. 시스템 운영 전에 설계 결함을 발견하기 위한 많은 절차들이 개발 프로세스에 설계되어 있다(또는 적어도 있어야 함). 이러한 절차가 왜 효과적이지 않았는지를 조사하는 것은 개발 과정의 지속적인 개선에 있어 중요한 요소이다.

## 시스템 이론 vs 복잡도 이론(Systems Theory vs. Complexity Theory)

STAMP는 복잡도 이론이 아닌 시스템 이론을 기반으로 한다. 많은 사람들이 시스템 이론에 기여해 왔지만 오스트리아의 생물학자인 베르탈란피(Ludwig von Bertalanffy)는 일반적인 시스템 이론의 창시자 중 한명으로 꼽힌다. 노버트 위너(Norbert Weiner)는 수학 및 공학에서의 의미를 연구하였다. 그의 이론은 *사이버네틱스(cybernetics)*라는 것인데 이 용어는 시간이 지남에 따라 사라졌고 베르탈란피의 용어가 오늘날 일반적으로 사용되고 있다.

이 핸드북 또는 다른 자료에서 볼 수 있는 시스템 이론은 자연적인 것이든 인공적인 시스템이든 간에 복잡한 시스템의 동작을 이해하는 데 사용될 수 있는 일련의 원칙이다. *시스템적 사고(systems thinking)*란 시스템 이론의 원칙을 적용할 때 사람들이 무엇을 하는지 설명하기 위해 자주 사용되는 용어이다. 이 원칙들은 본 핸드북 1장에 간략하게 기술되어 있다.

*복잡도 이론(complexity theory)*은 1960년대 시스템 이론 및 다른 개념에서 발전하였으며 일반적으로 산타페 연구소(Santa Fe Institute)와 그 곳에서 일한 연구원들과 관련되어 있다. 시스템 이론과 복잡도 이론 사이에는 몇 가지 공통점이 있다. 모두 발현(emergency)과 같은 용어를 사용하고 시스템을 컴포넌트로 환원하거나 분해하기보다는 전체로 간주하여 복잡한 시스템의 동작에 초점을 맞춘다는 점

of feedback and feedforward control, adaptability, nonlinear interactions, and constraints. Both reject reductionism or decomposition as a principle for understanding system behavior.

There are, however, significant differences. Complexity theory was created to describe natural systems where seemingly independent agents spontaneously order and reorder themselves into a coherent system using laws of nature that we do not yet fully understand. Systems theory, in contrast, is more appropriate for man-made and designed systems where the system is purposely created by humans using some engineering or design process and where the basic design is known and changes are controlled.

Another major difference is that systems theory considers all systems as displaying emergent behavior while complexity theory divides systems into four types: simple, complicated, complex, and chaotic, each with different degrees or types of emergence.

As such, systems theory appears to be most appropriate for engineered or designed systems while complexity theory is most appropriate for natural systems where the design is unknown, such as the weather, and for sociological systems, such as communities, that are not designed and where there is a lack of order and it is very hard or impossible to predict the emergent behavior. Complexity theory deals with behavior that cannot be designed but instead must be experienced and studied as it arises.

Systems theory, at least for me, is easier to understand and use. Complexity theory frameworks can be difficult and confusing to apply and understand and may be overkill for the engineering goals related to improving safety and other emergent system properties. For this reason, systems theory was selected as the basis for STAMP.

이 그것이다. 시스템 이론의 기본 컴포넌트는 발현, 계층구조, 커뮤니케이션, 컨트롤이며 이것은 복잡도 이론에도 포함된다. 시스템 이론과 복잡도 이론 모두 피드백과 피드포워드 컨트롤, 적응가능성, 비선형적 상호작용, 제약사항의 개념을 포함한다. 두 이론 모두 시스템의 동작을 이해하는 원칙으로 환원주의 또는 분해를 받아들이지 않는다.

그러나 중요한 차이점이 있다. 복잡도 이론은, 독립적으로 보이는 에이전트들이 우리가 아직 완전히 이해하지 못하는 자연의 법칙을 활용하여 스스로를 일관된 시스템으로 정렬하거나 재정렬하는 자연 시스템을 묘사하기 위해 만들어졌다. 반면, 시스템 이론은 사람이 만든 시스템에 보다 적합한 것이다. 여기서 시스템이란 엔지니어링 또는 설계 프로세스를 통해 사람이 의도를 가지고 만든 것으로 기본적인 설계를 알고 있으며 변경을 컨트롤 할 수 있다.

또 다른 중요한 차이점으로 시스템 이론은 모든 시스템이 발현적 동작(emergent behavior)을 보이는 것으로 간주하는 반면, 복잡도 이론은 시스템을 4가지 유형, 즉, 단순한(simple), 복합적인(complicated), 복잡한(complex), 혼란스러운(chaotic)으로 나눈다는 것이다. 각 유형은 각각 다른 정도 또는 각기 다른 유형의 발현 속성을 갖는다.

이와 같이 복잡도 이론은 날씨와 같이 설계를 알 수 없는 자연 시스템, 그리고 커뮤니티와 같이 설계되지 않았고 질서가 결여되어 발현적 동작을 예측하기 매우 어렵거나 불가능한 사회학적 시스템에 가장 적합하며, 시스템 이론은 엔지니어드 시스템 또는 설계된 시스템에 가장 적합한 것으로 보인다. 복잡도 이론은, 설계할 수는 없지만 대신 발생하였을 때 경험하고 학습해야 하는 동작을 다룬다.

적어도 본 저자에게 있어 시스템 이론은 이해하기 쉽고 사용하기 쉽다. 복잡도 이론의 프레임워크는 적용하거나 이해하기가 어렵고 애매모호하며 안전 개선 및 다른 시스템 발현 속성과 관련된 엔지니어링 목표를 달성하기에는 다소 무리가 있을 수 있다. 이러한 이유로 시스템 이론이 STAMP의 기반으로 선택되었다.

# CAST HANDBOOK

영문/한글판 v1.0

2020.12

발행처 : 한국정보통신기술협회

http://sw.tta.or.kr/notify/CASTHandbook(ENG_KOR).jsp