A new approach to prevent accidents in the steel industry

by

Paulo Francisco López De la Toba

B.S. in Mechanical Engineering with minor in Industrial Engineering
Instituto Tecnológico y de Estudios Superiores de Monterrey, México, 2006

Submitted to the System Design and Management Program
in partial fulfillment of the requirements for the degree of

Master of Science in Engineering and Management

at the

Massachusetts Institute of Technology

September 2019

© 2019 Paulo Francisco López De la Toba.
All rights reserved.

The author hereby grants to MIT permission to reproduce and to distribute publicly paper and electronic copies of this thesis document in whole or in part in any medium now known or hereafter created.

Signature of Author: _____

System Design and Management Program
August 16th, 2019

Certified by: _____

Dr. John P. Thomas
Thesis Supervisor
Research Engineer, Engineering Systems Laboratory
Safety and Cybersecurity Group

Accepted by: _____

Joan S. Rubin
Executive Director
System Design and Management Program

Page intentionally left blank

A new approach to prevent accidents in the steel industry

by

Paulo Francisco López De la Toba

Submitted to the System Design and Management Program
In Partial Fulfillment of the Requirements for the Degree of
Master of Science in Engineering and Management

Abstract

The steel industry has faced extraordinary changes over recent years incorporating new technologies and processes to make it more competitive and safer based on market requirements, regulations, and community concerns. Safety, in particular, has been an important topic in which the industry has put remarkable efforts to improve its performance.

Traditional safety models currently used to analyze and prevent accidents have been in use for decades. However, the complexity of systems has substantially increased over this time and has reshaped the way people perform their activities. The limitations of traditional models are becoming more evident as system complexity increases, especially when it comes to understanding the interactions between many system elements, incomplete or otherwise flawed requirements, design errors, and human behavior and contextual factors.

Today, there is general recognition that a new approach is needed to address the complexity of modern systems and to address the deeper systemic causes that are leading to accidents. This thesis evaluates and demonstrates how new approaches based on Systems-Theoretic Accident Model and Processes (STAMP) can be applied using a real case from the steel industry. Using these approaches, organizations can gain a broader perspective to understand the full range of factors contributing to accidents and create more effective measures to prevent future accidents.

This thesis examines a high-risk incident in a steel plant and compares a traditional Root Cause Analysis that was performed with a new systems approach called Causal Analysis based on System Theory (CAST). Causes and recommendations from both methods are compared. In addition, a systems approach for hazard analysis called Systems Theoretic Process Analysis (STPA) is evaluated to determine whether it could have anticipated the behaviors and contextual factors that led to the incident and whether it could have been prevented. These methods were found to be extremely effective in analyzing past accidents and in preventing future accidents, providing significant insights for organizations to understand the reasons behind accidents and to define the necessary steps to prevent them.

Thesis Supervisor: Dr. John Thomas

Title: Research Engineer, Engineering Systems Laboratory. Safety and Cybersecurity Group.

Acknowledgments

First, I would like to thank my advisor, Dr. John Thomas, for his enthusiasm, patience and guidance through this work. I am impressed by your vision and commitment to change the way people think about safety. Your passion was contagious, and it encouraged me to broaden my perspective about what we can do to prevent accidents. I highly appreciated your insights through this fantastic journey.

I want to thank my company for giving me the opportunity to pursue this dream. Particularly, I prize the support of Maximo Vedoya, Rodrigo Piña, Pablo Bassi, and Cesar Jimenez. Thank you for believing and placing your trust in me. I also acknowledge the candid and prompt support of Mario Resendez during my time abroad. Also, I thank all my work colleagues, especially to Eduardo Cabello, Raul Rosales, and Ricardo Ramirez, who provided countless insights that enriched this paper.

I cherish my friends for your dedicated support and caring through this experience. Particularly, to Jonathan and Jorge, thank you for all your thoughts, joy, and time during our time at MIT. To my lifelong friends, Jorge, Carlos, Memo, and Nino, thank you for standing by me through all these years. To my program colleagues and professors, thank you for blowing my mind, and nourishing me with all your enriched views. This year has been a vibrant, fun, and exciting time.

To my family. Thank you for always giving me your sincere support. Mom and dad, thank you for providing me the foundations of who I am today. You have been an enlightened compass guiding me in the chase of my goals and pushing me to aim high. To my brothers, thank you for being my lifetime and unconditional partners. I love you all. You have been my cornerstone all my life.

Finally, I would like to express my deepest gratitude to my wonderful wife, Patty. Without you, this project would not have had sense, and it would not have been possible. It has not been easy, but your lovely dedication, patience, and resilience have turned this journey into something memorable. Thank you for your infinite love. To my daughter, Ana Cristina, your smiles and laughs, and watching you grow have been my daily engine. Thank you both; you are my source of inspiration. This master is also yours.

Full Disclaimer: The opinions expressed in this thesis are those of the author and do not reflect the official policy or position of Ternium or other steel organization.

Table of Contents

List of Figures **8**
List of Tables **9**
Chapter 1: Introduction **11**
1.1 Motivation 11
1.2 Research Goals and Outline 13
Chapter 2: Background **14**
2.1 Steel Industry Overview 14
2.2 Safety in the Steel Industry 15
2.3 Company overview 17
Chapter 3: Literature Review **19**
3.1 Traditional accident models 19
3.1.1 Domino Accident Model and the Swiss Cheese Model 19
3.1.2 Root Cause Analysis 21
3.2 Traditional Hazard Analysis Methods 23
3.2.1 HAZOP 23
3.2.2 Bow Tie 26
3.3 STAMP: A new accident causality model 28
3.3.1 CAST: accident analysis 32
3.3.2 STPA: hazard analysis 34
3.4 Summary of literature review. Comparison between models 35
Chapter 4: A case study in the steel industry **38**
4.1 Steel Making Overview 38
4.2 Case Study Incident 44
4.3 Root Cause Analysis performed by the company 48
4.4 CAST Analysis 53
4.4.1 Identify the system 53
4.4.2 Identify the losses, hazards and safety constraints 53
4.4.3 Safety control structure 54
4.4.4 Proximal events leading to the loss 63
4.4.5 Analysis of the loss at a physical system level 64
4.4.6 Analysis of the loss at the control system level 66
4.4.7 Coordination and communication contributors 101
4.4.8 Dynamics and changes in the system over time 104
4.4.9 Recommendations 106
4.4.10 Additional facts uncovered while applying CAST 112
Chapter 5: Comparison between CAST and Root Cause Analysis **114**
5.1 Classification of causes 114

5.2 Analysis of Results 130
Chapter 6: Could these type of accidents be prevented? 134
6.1 STPA: Define the purpose of analysis 134
6.2 Model Control Structure 136
6.3 Identifying Unsafe Control Actions 139
6.3.1 Identifying Accident Scenarios 140
6.3.2 Safety Requirements 148
6.4 Discussion of STPA Process and Results 151
6.5 Could the STPA approach work if someone does not know the event and is not an expert in STPA? 152
Chapter 7: Conclusions 155
7.1 Conclusions and Recommendations 155
7.2 Suggested implementation roadmap of STAMP in large organizations 157
7.3 Future work 158
References 158
Appendix 1: Interactions in safety control structure. Safety Team & Corporate Management 161
Appendix 2: Interactions in safety control structure. Operations Team. 162
Appendix 3: Interactions in safety control structure. Maintenance Team. 163
Appendix 4: Interactions in safety control structure. Engineering Team. 164
Appendix 5: STPA Unsafe Control Actions 165

List of Figures

Figure 1: worldsteel safety and health principles and activities [2] 16
Figure 2: Global Lost Time Injury Frequency Rate in steel industry [2] 17
Figure 3: Henrich's Domino Accident Model [7] 20
Figure 4: Swiss Cheese Model [8] 21
Figure 5: Root Cause Analysis Tree Diagram. Extracted and adapted from [10] 22
Figure 6: Flow diagram of the HAZOP examination stage [12] 25
Figure 7: Bow Tie Model [27] 27
Figure 8: Differentiation between STAMP and traditional safety models based on events [24] 29
Figure 9: Relationship between system, subsystems and environment [15] 30
Figure 10: Interactions between different control levels [3] 30
Figure 11: Generic example of a hierarchical control structure [3] 31
Figure 12: Representation of process models [3] 32
Figure 13: Steelmaking flow sheet [16]. The encircled process corresponds to the electric arc furnace 39
Figure 14: Vertical section of EAF shop [16] 40
Figure 15: Current EAF standard design [16] 41
Figure 16: Example of water panels and their distribution over the sidewalls and the roof of a furnace [16] 42
Figure 18: Electric Arc Furnace Operation 43
Figure 19: Fuchs electric arc furnace 45
Figure 20: The moment when the electrode's lift plug broke 45
Figure 21: The lift plug fell towards the water piping over the furnace roof 46
Figure 22: The lift plug hit the water piping over the furnace roof 46
Figure 23: Water leak due to the damage of water piping 46
Figure 24: Electrode is damaged by the furnace roof while opening it 47
Figure 25: Root cause analysis of the first reaction performed by the company 49
Figure 26: Root cause of the second reaction performed by the company 50
Figure 27: Level 1 high-level safety control structure 55
Figure 28: Level 2 high-level safety control structure 56
Figure 29: Detailed engineering safety control structure 58
Figure 30: Safety control structure for operations and maintenance 61
Figure 31: DSM of safety control structure 62
Figure 32: UCAs at the lower organizational level 97
Figure 33: UCAs at the medium organizational level 98
Figure 34: UCAs at the upper organizational level 99
Figure 35: Communication links in the system 102
Figure 36: Extract of control structure of operations and maintenance team from Figure 30 103
Figure 37: Graphic representation of number of causes and factors detected by model 131
Figure 38: High-Level Safety control structure at operational level 136
Figure 39: Detailed safety control structure for systems controlled by the control room operator 137
Figure 40: Subsystem considered for the STPA analysis 138
Figure 41: Fuchs furnace components and its movements 139
Figure 42: Detail of control structure for the selected UCAs 141

Figure 43: Distribution of recommendations according to the safety hierarchy of control. Modified from [28] 151

List of Tables

Table 1: Typical HAZOP template [12] 26
Table 2: Example of a UCA table 35
Table 3: Comparison between accident models 36
Table 4: Comparison between accident analysis techniques 36
Table 5: Comparison between hazard analysis techniques 37
Table 6: Analysis of loss at the control system level. Plant Operators 67
Table 7: Analysis of loss at the control system level. Operations Engineers and Supervisors 70
Table 8: Analysis of loss at the control system level. Operations management 74
Table 9: Analysis of loss at the control system level. Maintenance technicians and contractors 78
Table 10: Analysis of loss at the control system level. Maintenance leaders and supervisors 79
Table 11: Analysis of loss at the control system level. Maintenance management 81
Table 12: Analysis of loss at the control system level. Engineering worker 83
Table 13: Analysis of loss at the control system level. Project manager 85
Table 14: Analysis of loss at the control system level. Engineering management 87
Table 15: Analysis of loss at the control system level. Safety engineer 89
Table 16: Analysis of loss at the control system level. Safety management 91
Table 17: Analysis of loss at the control system level. Corporate management 95
Table 18: Recommendations for physical equipment and system design 106
Table 19: Recommendations for procedures and routines 107
Table 20: General recommendations 107
Table 21: Specific recommendations to operations team 110
Table 22: Specific recommendations to maintenance team 110
Table 23: Specific recommendations to engineering team 110
Table 24: Specific recommendations to safety team 111
Table 25: Specific recommendations to corporate team 111
Table 26: Comparison of factors detected between the RCA performed by the company and CAST, taking RCA as baseline 115
Table 27: Comparison between CAST and RCA performed by the company, taking CAST as baseline 116
Table 28: Selected UCAs to perform the STPA Analysis 140
Table 29: UCAs identified by participants in STPA tests 153

Page intentionally left blank

Chapter 1: Introduction

1.1 Motivation

"Nothing is more important than the safety and health of the people who work in the steel industry."

worldsteel Board of Directors

The world has experienced changes in recent years at a speed never seen in human history. The advancement of technology is re-shaping the way we interact with each other and has created both new businesses and new ways to manufacture products. However, ability to fully understand all the implications that come with these accelerating technological changes has not kept pace [1].

The steel industry has not been a stranger to these changes. New technologies have emerged to improve the productivity and cost-efficiency of companies to sustain their competitiveness in the tight steel market. This technology evolution has brought new challenges crucial for safety management.

While it is evident that safety metrics in the steel industry have been improving over the last few years at a macro-level [2], high-risk incidents and accidents continue to be a reality in the industry. One of the underlying problems is that while technology has evolved rapidly and changed the safety dynamics, the models to analyze them have not evolved to keep pace with the new reality [3].

Traditional causality models and hazard techniques were created many decades ago when automation and systems complexity were at a very different level than they are today. These models use a linear causality perspective, usually focusing on physical causes or operator responsibility for safety without taking into consideration other significant factors such as the interaction between elements and subsystems, flawed assumptions, design and operations reviews that were intended to prevent accidents, or the context that helped induce unsafe operator or automation behavior. These factors have an important influence on the safety dynamics and deserve to be studied in detail.

High-risk accidents and incidents in the last years have shown us that typically systematic and structural deficiencies are the underlying causes of accidents [3]. Meanwhile, we tend to focus

on unsafe actions and component failures simply because they are easier to detect. This makes it easy to cast blame and assigned punitive measures in an effort avoid its recurrence. Nevertheless, these conditions might be only superficial symptoms of the true root causes that are not evident at first sight. We need new methods to perceive and understand what might not be immediately visible.

At the same time, communities have become more concerned and aware about industrial safety. They have played an active role demanding stiffer regulations to the industry, and good principles of social responsibility. The steel industry has acknowledged this situation, and safety has become a paramount as a matter of business sustainability. This industrial sector traditionally has had a reputation as a high-risk and unsafe activity. While it is true that it could be considered as a high-risk industry, this does not mean it has to be unsafe. The steel industry has been working hard to improve this perception, establishing an evident commitment to improving safety conditions and applying standardized procedures and best practices to improve safety performance.

Some companies are leading the initiative to transform the perception of the steel industry regarding safety. One of these companies is the object of this thesis. The company has had an outstanding improvement record in its safety figures, and it is a safety reference for the industry in Latin America. However, although its statistics reflect a significant improvement over the years, the company's efforts have not been enough to prevent high-risk accidents and incidents.

Those are some of the reasons why a new safety approach is needed. STAMP (Systems Theoretical Accident Model and Processes), is a new model that provides a systematic way to understand safety with a holistic view. This method provides a useful framework to understand the causality of safety events in complex systems in a comprehensive way.

STAMP is a promising tool that is experiencing a rapid adoption in other industries including automotive, aerospace, aeronautics, nuclear power, chemical, oil & gas, and others due to its systemic approach. In contrast to traditional failure-based models, STAMP views safety as a control problem requiring the enforcement of constraints to prevent accidents. Although STAMP is undergoing rapid adoption in other industries, at the time of this writing there is no record of a formal comparison between traditional methods and STAMP in the steel industry. This thesis aims to provide the first formal comparison in the steel industry.

This thesis evaluates STAMP as a modern alternative to address the gap of traditional models in the steel industry. By using a real industry case study, this thesis evaluates the benefits of using a systematic approach to understand the safety dynamics of organizations and

processes in contrast to the outcomes from traditional methods. Finally, this work proposes recommendations about how to implement STAMP in companies where other models and tools are currently in use.

1.2 Research Goals and Outline

The goals of this thesis are:

1. Evaluate the strengths and limitations of traditional causality models and hazard methods compared to STAMP to analyze and prevent accidents.
2. To evaluate STAMP-based methods in their ability to analyze and potentially prevent a high-risk incident in the steel industry.
3. To compare and contrast STAMP-based methods against the traditional analysis performed by the company.

This thesis is divided into seven chapters. Chapter 1 provides the motivation and research goals of the thesis. Chapter 2 presents a brief background of the steel industry and an overview of the company in which the analysis was conducted.

Chapter 3 describes the fundamentals of some of the most common accident models and hazard techniques, as well as their advantages and disadvantages. Also, it introduces STAMP and its techniques to analyze accidents (CAST) and hazards (STPA). Chapter 4 explains the manufacturing process of steelmaking and the details of the case study incident. It also presents the traditional analysis of the event performed by the company, and it shows a detailed CAST analysis of the same event. Chapter 5 describes the identified gaps between the analysis performed by the company and CAST.

Chapter 6 aims to answer the question of whether this type of safety event could be avoided. The chapter proposes a STPA analysis creating different scenarios that may lead to a mishap. Also, it shows the results of an experiment conducted to understand how challenging it could be to apply this methodology to with people who are not familiar with the event.

Finally, Chapter 7 provides conclusive insights about this thesis and a suggested roadmap to implement this model in large companies.

Chapter 2: Background

This chapter provides a general overview of the steel industry. It describes the relevance of the industry and their efforts regarding safety management. Also, it provides a background of the company in which this thesis was conducted.

2.1 Steel Industry Overview

Steel has been an essential part of human history during the past few centuries. Since our first contact with iron in the 13th century B.C., humankind has been interested in the development of new processes to take advantage of the characteristics of this metal.

While it is true that we can trace the beginning of steelmaking to centuries past, the industrialization of steel began in the Industrial Revolution. This is due to the Bessemer process and Siemens's open-hearth process in the 1850s [4]. These technologies enabled the mass production of steel and played a fundamental role in the war period during the first half of the 20th century.

After World War 2, the world had a robust economic expansion, and with that appeared new needs from the global population. These needs were satisfied by the industry. At that time, new technologies in power generation and transmission had a substantial effect on the falling cost of electricity, enabling the emergence of new technologies to produce steel at a cheaper cost. These processes include the Electric Arc Furnace and the Continuous Casting process. Later, this price advantage leveraged the development of a breakthrough process for steel production such as the Mini-Mills in the early 1970s.

Nowadays, steel is the most widely used and the most recycled metal in the world. The steel industry is one of the largest in the world, with revenues above US $1380 billion per year, and more than 6 million direct employees globally [5]. Steel is a versatile material with broad applications, such as buildings and infrastructure, car manufacturing, metal products, mechanical equipment, home appliances, and other usages.

The steel production has two possible process pathways, the Basic Oxygen Furnace (BOF) or the Electric Arc Furnace (EAF). In the BOF production process, steel is produced from raw materials like iron ore, coke, and limestone, in addition to a small amount of old steel (scrap). On the other hand, in the EAF process, steel could be produced from 100% recycled scrap or in combination with direct-reduced iron pellets. This production process has several steps,

including furnace charging, melting, refining, de-slagging, tapping, and, finally, furnace turnarounds. The steel produced from either process is then cast into various shapes according to the requirements of its consumers.

Over the last decades, the industry has experienced drastic changes. The industry has incorporated new technologies to improve its efficiency, environmental footprint, and safety, with new market conditions and stringent regulations. Automation has been an essential tool throughout this process. It has relieved workers from hazardous and extenuated activities and has been an essential support to actively monitoring complex processes. However, human operators continue to be a critical component of the production system in supervisory and monitoring roles.

The adoption of new technologies will continue to be a trend in the industry in the coming years. Meanwhile, the workers will require more cognitive skills and abilities to face these future changes.

2.2 Safety in the Steel Industry

The steel industry has been traditionally perceived as a dangerous activity where accidents were inevitable and intrinsically related to the process. This old paradigm has resonated for many years in our societies and has created a bad reputation for the industry. Nevertheless, the steel industry has acknowledged this issue and has put much effort during the last years to overcome this situation.

World Steel Association (WSA) is the global organization that represents steel producers, national and regional steel industry associations, and steel research institutes. It has played an active role to ensure constant improvement in industry safety. The institution has set guidelines and defined the best safety practices to its members. Related to the latter, WSA defined six principles to outline this philosophy [2]:

1. All injuries and work-related illness can and must be prevented.
2. Management is responsible and accountable for safety and health performance.
3. Employee engagement and training is essential.
4. Working safely is a condition of employment.
5. Excellence in safety and health supports excellent business results.
6. Safety and health must be integrated into all business management processes.

These principles are matched with a series of activities to promote an accident-free workplace (shown in the outer ring in the next figure).



Figure 1: worldsteel safety and health principles and activities [2]

WSA defined three areas to manage safety comprehensively:

- **Occupational Safety Management**: focus on primary prevention of exposure to hazards.

- **Occupational Health Management**: focus on long-term effects on exposure to hazards encompassing the physical, mental, and social well-being of people working in the industry.

- **Process Safety Management**: focus on preventing catastrophic accidents and incidents from protecting not only the people within the company but also including the environment, assets, and community.

These strategies have generated significant improvements in the aggregate safety metrics of the steel industry, as shown in the next chart:

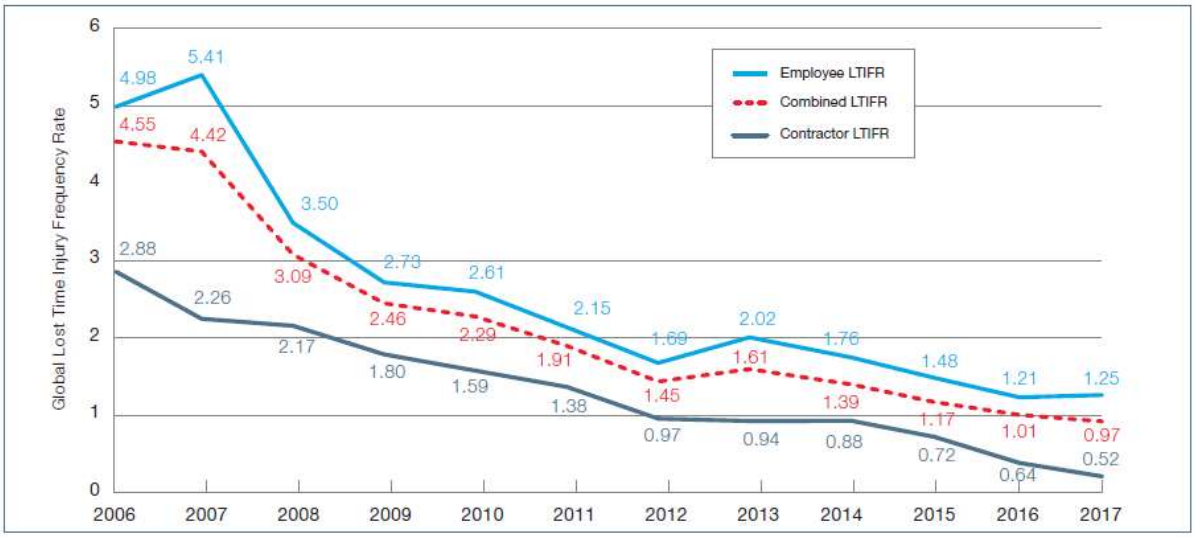


Figure 2: Global Lost Time Injury Frequency Rate in steel industry [2]

The Lost Time Injury Frequency Rate corresponds to the number of accidents that causes injuries preventing the person from returning to his next scheduled shift or work period (including fatalities), per million person-hours. This metric has decreased from 4.55 in 2006 to 0.97 in 2017, a substantial reduction of 78.67% [2].

It is evident that there has been a significant improvement in the aggregate metrics over the last few years. However, WSA recognized there are still opportunities to improve as safety is a never-ending effort.

2.3 Company overview

The company in which this thesis was conducted is the steel leading manufacturer in the Americas. It supplies a broad range of steel products to varied industries such as construction, automotive, home appliances, energy and transport in all the main markets in the region.

The organization has a highly integrated production system, from the mining of iron ore to the production of high value-added products. It has several production centers located mainly in Latin-America. The company stands out due to its broad product portfolio, as well as the strength of its service and distribution centers network, which allows it to be close to its customers all along the Americas.

The corporation has a robust technical culture, industrial vocation, and long-term view. This envisioning strides with a strong commitment to excellence in safety. Since the foundation of the company, essential milestones regarding safety have occurred, helping to consolidate the vision of management about safety.

In 2010, the company launched an ambitious program called Safety First to cultivate a more comprehensive safety culture through numerous initiatives. One of the pillar activities of the program is the Safety Hour, where operations management at all levels visit the facilities with the sole intention to have a positive approach with workers to understand their safety concerns, detect potential risks and unsafe behaviors. This opportunity fosters open communication and empathy through the company, giving a chance for management to obtain insights directly from the floor.

In 2013, the company adopted Root Cause Analysis as the standard model to analyze the safety events in their operations, focusing on three significant causalities: physical conditions, human error, and structural/systemic anomalies. However, in July 2013, despite the company's efforts regarding safety, a tragic accident occurred in one of its plants in Mexico where regrettably several employees perished. This was the worst accident in company history, and it shocked the company to its foundations. This event was a critical turning point for the company; it prompted a renewed commitment to improving safety performance and increasing awareness. The company launched several investments to improve safety conditions across their plants focusing in the high-risk operations; this process was bolstered by a new extended approach to consider safety process management as a core part of its operations.

In 2016, the organization summarized the main principles of the Safety-First program by listing ten actions, the Ten Life Saving Rules, that everyone in the company should follow to avoid accidents. These rules were defined according to the leading causes of risk in operations, and they reflect the scope of safety regulations in the countries where the company has operations.

The benefits from all these initiatives are manifested in the company’s safety indicators, which have significantly improved after the tragic accident in 2013. The company results in safety compare well to the references from the WSA. However, the broader issue of safety involves more than just occupational safety indicators, as management strives to foster a corporate culture embodying values centered on safety as an integral part of its everyday life.

Chapter 3: Literature Review

This chapter reviews traditional approaches to safety, including their strengths and limitations regarding the evaluation of complex systems. This chapter also discusses STAMP, a new model helpful to understand complex systems and to overcome the shortcomings from traditional models.

3.1 Traditional accident models

Traditional safety models take a linear causality view of accidents, where each failure is the direct cause of the next event in the chain and can be traced back to a root cause. Accidents are considered as a sequence of events over time and generally, are energy-related or involve deficiencies in physical conditions (component failures) or human error.

3.1.1 Domino Accident Model and the Swiss Cheese Model

In 1931 Herbert Henrich proposed the Domino Accident Model, based on his own experience in the industry. At that time, thanks to electrification, machines were able to be designed to perform more complex activities that had previously been done by humans. The concept of safety management was at a rudimentary stage, and the causes of most accidents were assigned to physical causes, such as lack of equipment guards.

Henrich introduced the idea of man failure as the principal cause of injury. According to his experience in the industry, most accidents (88%), were related to unsafe acts, 10% to unsafe conditions, and 2% to acts of God.

“Faulty instruction, lax discipline, unsafe practices, inattention, and physical and mental impairment or inefficiency are some of the real causes of construction accidents, and they produce 88 percent of all injuries [7]”.

It is important to note that Henrich never published the data considered to formulate this approach; therefore, it is not possible to verify the figures he affirmed to support his causality model.

Under this context, Henrich created his approach considering five stages in an industrial accident, as shown in the following figure:

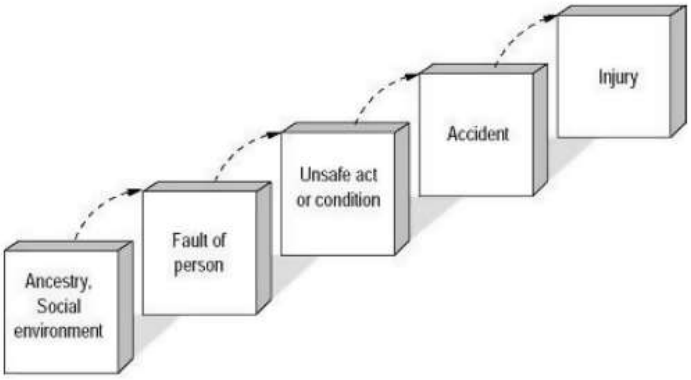


Figure 3: Henrich's Domino Accident Model [7]

According to his model, accidents occur as a sequence of colliding dominoes; hence, if one of the dominoes is removed, the chain could be interrupted, preventing an accident. Since the model proposed that most of the accidents are human related, the focus should be to prevent unsafe acts or conditions. Henrich suggested that to overcome this situation, it was necessary to enforce supervision, training, and discipline.

This model became popular due to its simplicity and perhaps due to our inherent tendency to assign blame; in fact, many of its assertions still persist in some industries today. While it could be true that some accidents may have a component of lack of discipline or inadequate supervision, this view also may oversimplifies the full range of factors involved and can obscure the underlying causes of accidents.

Nevertheless, as mentioned before, the Domino model emerged as an authoritative reference for many decades and influenced other safety approaches.

In the late 1980s, James Reason proposed the Swiss Cheese model, incorporating the idea of layers of defense or protection. This model argued that accidents could be caused by failures in four planes lying one behind the other: 1) organizational influences; 2) unsafe supervision; 3) preconditions for unsafe acts; 4) unsafe acts [8].

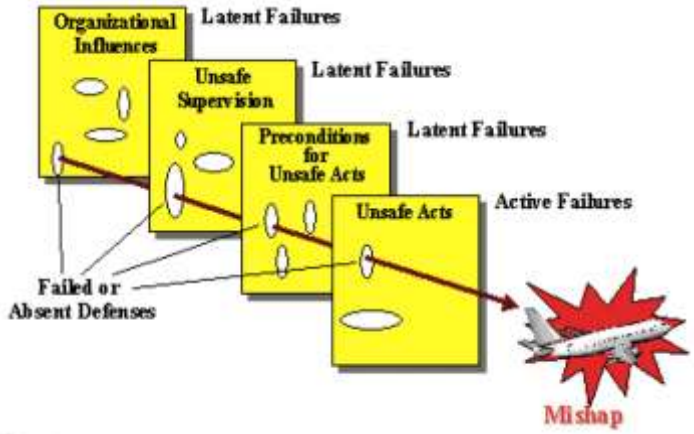


Figure 4: Swiss Cheese Model [8]

Each of these stages is represented as a slice of “Swiss Cheese”, where the holes are defects or vulnerabilities randomly changing in location and size. Eventually, the trajectory of the hazard finds a clear pathway through all the layers leading to a failure (accident). This assumption conveys the idea that a single failure, whether technical or human, is insufficient to cause an accident.

This model focuses on individual layers to avoid the possibility of an accident. However, it does not take into consideration the systematic causes that might affect multiple layers simultaneously, for example, inadequate communication or poor safety culture within the organization. Like the Domino model, this model tends to oversimplify the dynamics of complex systems in which components cannot be treated as independent or isolated.

3.1.2 Root Cause Analysis

This method seeks to identify the underlying causes that contribute to the occurrence of an event rather than the generalized or immediate factors. The origins of the Root Cause Analysis (RCA) could be traced back to 1950s in Japan, where Sakichi Toyoda implemented this method for quality purposes in manufacturing. RCA evolved over time and expanded its applicability to other fields, including safety, to analyze root causes effectively.

According to the guidelines specified by the Department of Energy (DOE), the process to perform an RCA should include five phases [9]:

1. Data collection: The information to be gathered should consist of conditions before, during, and after the occurrence, and relevant information about the event.

2. Assessment:

2.1 Identify the problem

2.2 Determine the significance of the problem

2.3 Identify causes (conditions and actions) immediately preceding the event

2.4. Traced back precedent causes.

3. Identify recommendations to eliminate or mitigate the event

4. Inform: communicate the findings to avoid future events

5. Follow up: effectiveness review to detect if the corrective actions have been implemented and are preventing a recurrence.

One of the most common graphical techniques to perform this analysis is the Causal Factor Tree Analysis. This method displays in a structured hierarchy through cause-effect branches, the conditions that were necessary to occur an event. This representation usually is easy to follow and understand and has become one of the most popular investigation tools nowadays.

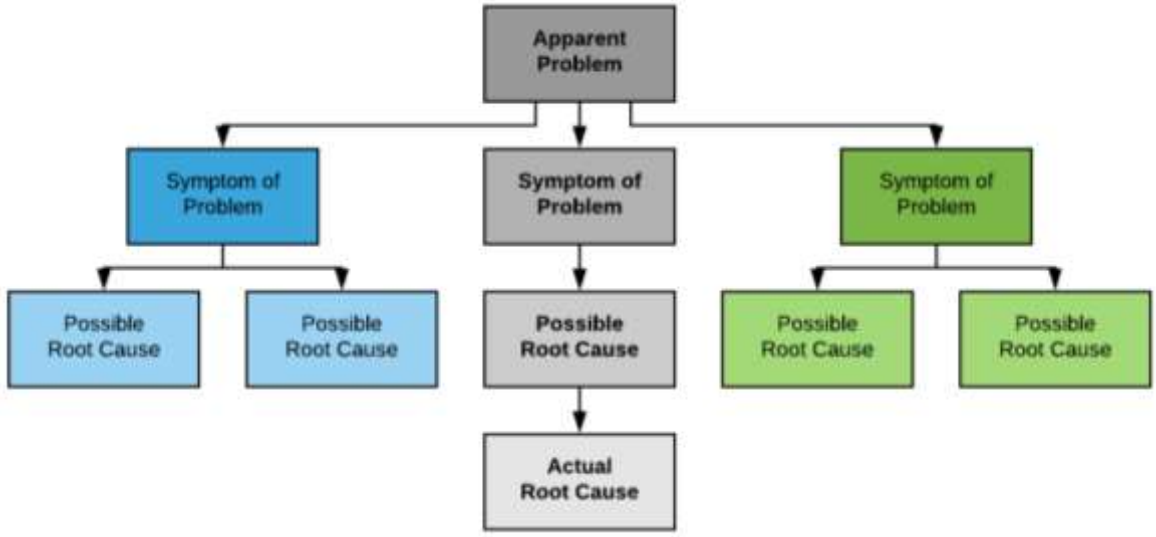


Figure 5: Root Cause Analysis Tree Diagram. Extracted and adapted from [10]

The chain of causes and effects generally flows from bottom to top. The objective of the RCA is to decompose the event and reach to the core of the problem. The more in-depth the analysis of the causal chain, the greater the influence of the corrective action may have in the whole system.

One of the shortcomings of this technique is that it provides a structure for organizing the causes that are known and identified but it does not provide a systematic method to carefully identify all causes and ensure that important causes are not missed. Sometimes it is not possible to identify an immediate cause for an element in the tree; in that case it may not provide the tools to adequately solve the problem.

The Root Causes Analysis method suggests that all undesirable outcomes are related to [11]:

- Physical roots: related to failure components.
- Human roots: actions or inactions that trigger the events.
- Latent roots: organizational systems that are flawed.

This method requires personnel with expertise in the field. The potential issue with this is that the expert could be biased towards a favorite cause and overlook some other potential causes. Therefore, a broader perspective is required to identify unrelated problems since this method does not clearly illustrate the relationships and interactions between causal factors. Single dependencies between factors are easy to represent with this kind of diagrams; however, complex systems and more elaborate dependencies become challenging to illustrate. While linear relationships can be shown (downward arrows in the tree diagram above), feedback, control loops, and other non-linear relationships are omitted.

Finally, another significant limitation is lack of a clear stopping rule. The analysis goes backward until an arbitrary stopping point. There is no specific rule about when to end the analysis; therefore, it typically continues until a convenient or most likely cause is reached that satisfies the biases or expectations of the analyst or management.

3.2 Traditional Hazard Analysis Methods

In order to prevent future accidents and to understand the full range of potential causes that may lead to a safety event, it is important to consider other analysis methods. The following section briefly describes the most common hazard technique used nowadays.

3.2.1 HAZOP

The Hazard and Operability Study (HAZOP) was developed during the 1960s by the Heavy Organic Chemical Division of the Imperial Chemical Industries (ICI). The ICI created a standardized method of analyzing processing hazards by starting with the basic operating conditions and then changing individual parameters one at a time to determine the subsequent consequences.

Although the technique was developed during the 1960s, it started to be widely used within the chemical process industry after the Flixborough, UK disaster in 1974 where several people perished, and numbers were seriously injured. This event raised a red flag in both the industry

and society about the relevance of process safety and the need to have a more systematic approach about it.

A HAZOP study is a structured technique for system examination and risk management, usually carried out by a multidisciplinary team. HAZOP relies on the experience and judgment of the team analyzing the system; thus, it is essential to have the participation of specialists with knowledge of system deviations. This technique is based on a theory that assumes deviations from design or operating intentions cause risks events. To identify such deviations, a set of guidewords is used in combination with the system parameters to recognize significant deviations from the design intention [12].

Some common HAZOP guide words to help identify potential deviations include:

- No or not
- More / Less
- As well as
- Part of
- Other than / instead
- Reverse (of intent)
- Early / Late
- Before / After

The analysis is carried out on all relevant elements. To facilitate the analysis, the system is decomposed into simpler sections called nodes to be individually reviewed. The extent of the nodes should be appropriate to the complexity of the system and the magnitude of the hazards in order to perform a meaningful analysis.

The HAZOP guidewords are then applied to each of these elements in a systematic way to identify possible deviations that are credible, and that could lead to potential hazards to safety, health, or environment.

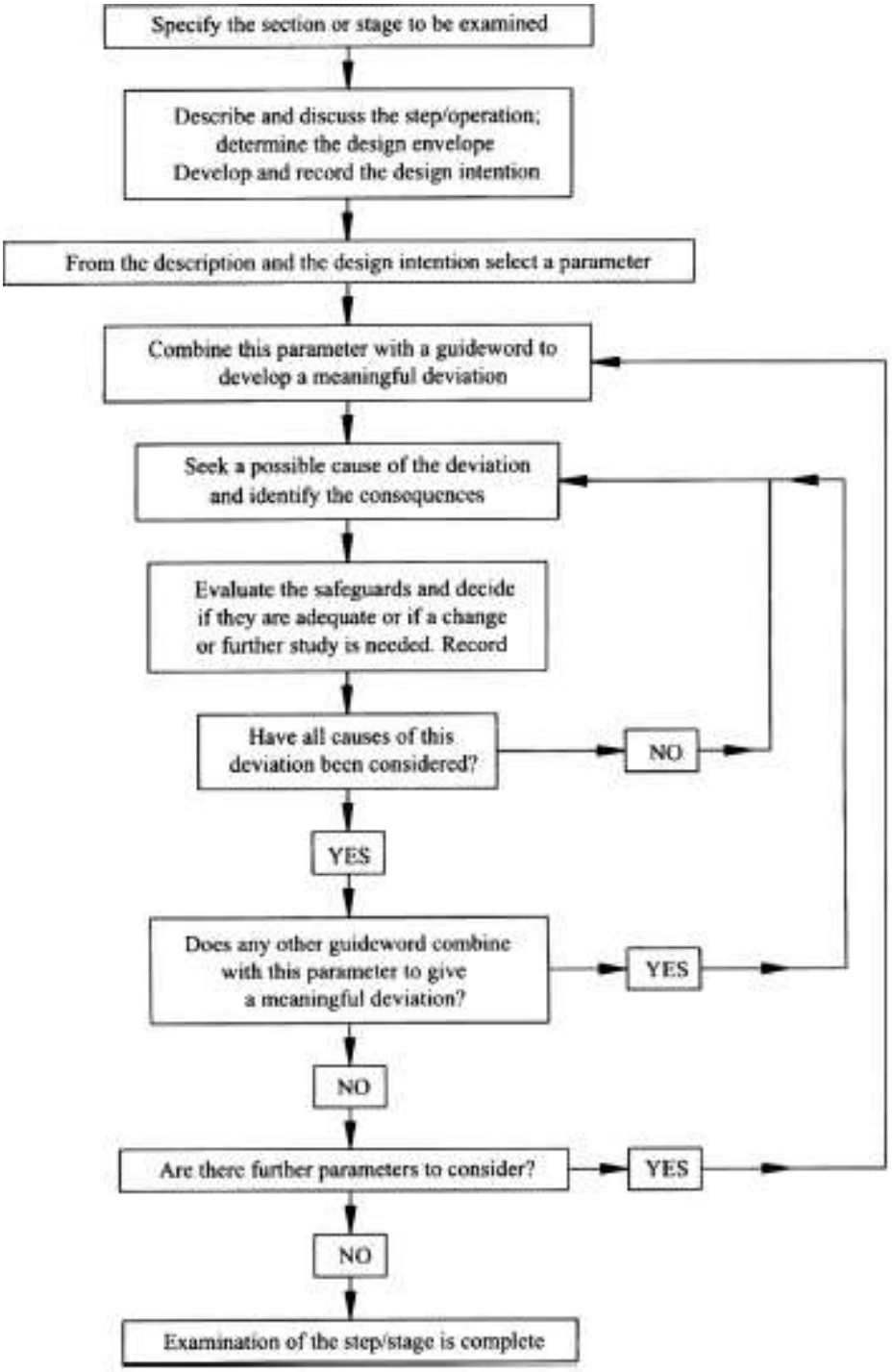


Figure 6: Flow diagram of the HAZOP examination stage [12]

Once the deviations are found, their causes and consequences need to be addressed. If the existing protection layers or safety measures are considered as deficient, then the team recommends action for change or calls for further investigation of the problem.

Table 1: Typical HAZOP template [12]

No.	Guide Word	Element	Deviation	Possible Causes	Consequences	Safeguards	Comments	Actions Required	Actions Assigned to
Assign each entry a unique tracking number	Insert deviation guide word used	Describe what the guide word pertains to (material, process step, etc.)	Describe the deviation	Describe how the deviation may occur	Describe what may happen if the deviation occurs	List controls (preventive or reactive) that reduce deviation likelihood or severity	Capture key relevant rationale, assumptions, data, etc.	Identify any hazard mitigation or control actions required	Record who is responsible for actions

HAZOP has been commonly used in the industry to analyze process safety; however, several extensions have been developed to address the human and software behavior [13]. Human-HAZOP variants have been developed to study human deviations from procedures. The framework of the analysis is similar, using guidewords to identify the possible deviations in procedures that may lead to an accident. However, this approach does not consider the underlying reasons that explain why a person believes that decision was suitable at that moment, and may not consider the overall context and design flaws that may lead to an accident [14]. These factors are critical in understanding and preventing accidents in complex systems.

A HAZOP study typically is qualitative and relies on the judgment and experience of the team participating; thus, expertise is crucial to the quality and completeness of a study. The accuracy and availability of the information to perform the analysis are defining factors for a meaningful analysis.

This technique has been widely used in the industry for many years and has become a reference for hazard analysis. Its methodology is relatively intuitive and straightforward to follow, and currently, software is available to assist its execution. However, the methodology has some limitations, such as the lack of assessing hazards involving many interactions between elements of the system, the oversimplification of human behavior and contextual influences, and the dynamics of the overall system (not just individual elements).

Similarly, HAZOP has been criticized for its ambiguity, incompleteness, nonsensicality, inefficiency, and redundancy while used to analyze software [20]. The analysis process becomes very complex and time-consuming for complex systems with a significant amount of data flow.

3.2.2 Bow Tie

Another method that has been commonly used in the industry is the Bow Tie. This method gets its name from its appearance, which resembles a man’s bow tie. The origin of this methodology is uncertain, but the first documented appearances come from courses notes of the Imperial Chemical Industries (ICI) at the Queensland University, Australia in 1979. The Oil

and Gas industry, particularly the Shell group, were early adopters of this approach to analyze and manage risks, and have integrated it for decades into its business practices.

This method intends to provide a summary of plausible scenarios that may lead to a hazard, and the safety barriers the organizations should consider to prevent and mitigate these scenarios. Once the barriers have been identified, the organizations need to identify the ways these barriers could fail.

A bow tie diagram includes the following elements [27]:

- **Hazard:** the state or source of potential damage. This element is the central part of the analysis.
- **Top event:** the situation or moment when the control over the hazard is loss.
- **Consequences** of the loss of control, which are the unwanted outcomes that the top event could lead.
- **Threats:** they are the possible cause that could trigger the occurrence of the top event.
- **Prevention barriers:** they are the measures that could be taken to stop and prevent threats.
- **Mitigation barriers** to stop or reduce the impact of the top event.
- **Degradation factors** which could lead to the failure or impairment of the prevention barriers.
- **Degradation controls** to keep the intended function and effectiveness of the prevention barriers.

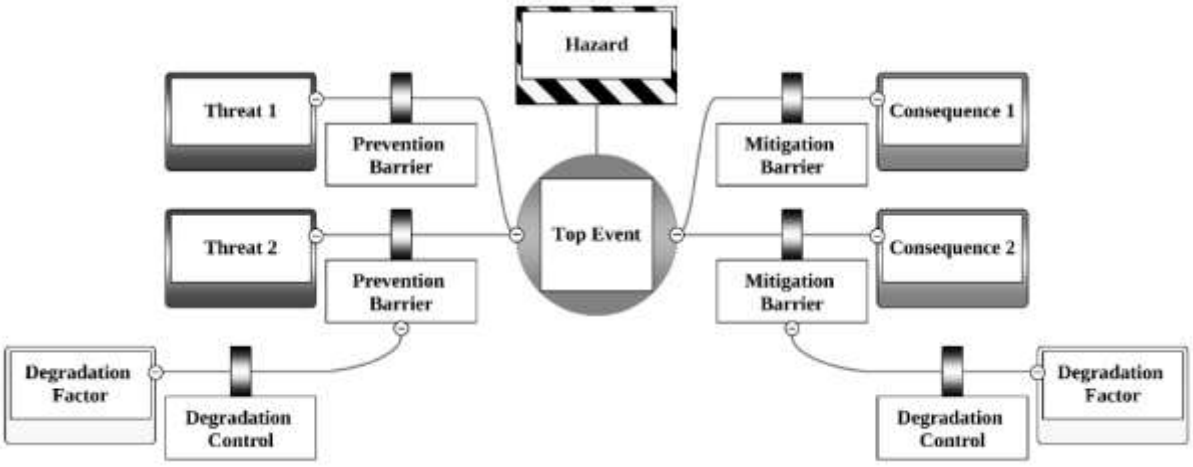


Figure 7: Bow Tie Model [27]

The bow tie analysis provides a big picture of the dynamics of safety, helping the organizations to focus on the barriers and controls that are required to prevent the occurrence of the top

event. This method has been used in the process industry, mainly on the prevention of Major Accident Events as it emphasizes on barriers and controls.

The graphical representation of the model provides an effective way to understand the possible causes and consequence of an analyzed event, and what could be the controls the organization needs to ensure to prevent its occurrence. As it is visually easy to follow, the model is a good tool to communicate the risks and the required control measures to maintain a system safe state. The method has software support to create the diagrams and to perform the analysis, which could be helpful to simplify the study process.

Perhaps, one of the main limitations of this model is that it does not provide a structured framework to identify the plausible causes and consequences related to the top event. The avoidance of omissions and a good understanding of the cause-effect rely on the knowledge and expertise from the people performing the analysis. Additionally, the model does not provide a quantitative assessment to evaluate the system. However, the method has proved to be a relevant tool for the industry for its good trade-off between its capabilities and its ease to perform the analyses.

3.3 STAMP: A new accident causality model

Traditional accident models have been challenged by the advancement of technology and the increasing complexity of sociotechnical systems. The interaction between humans and machines have changed in the last few decades, with more complex software systems and more sophisticated equipment. Many are finding the traditional safety approaches to be no longer adequate.

STAMP (Systems-Theoretical Accident Model and Processes) is a causality model introduced by Leveson in 2002. This approach addresses gaps in traditional safety models that assume accidents arise from linear chains of failures. Instead, STAMP is based on system theory and considers safety as an emergent property arising from the interactions among the system components. According to systems theory, to control the emergent properties it is necessary to impose constraints on the behavior and interactions between components. Hence, safety becomes a control problem that requires the enforcement of constraints [3].

As a systemic approach, this model has a broader vision to understand the accident causality in complex systems by identifying more causal factors such as organizational structures, human decision-making, human factors, design and requirements flaws, and the interactions between all elements.

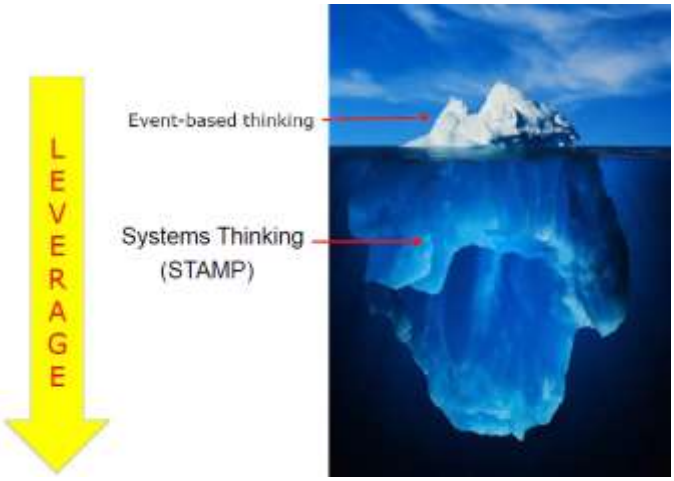


Figure 8: Differentiation between STAMP and traditional safety models based on events [24]

Understanding the causes of an accident requires determining why the control structure was not adequate to enforce the necessary constraints, and what is needed to prevent future accidents.

The STAMP framework serves as the basis for several methods. The most popular are CAST (Causal Analysis using System Theory) and STPA (System-Theoretic Process Analysis):

- CAST: a retroactive method to study accidents or incidents that have occurred and their causal factors.
- STPA: a proactive analysis method to analyze the potential causes of future accidents so hazards can be eliminated or controlled.

The following sections describe the fundamentals of STAMP, CAST, and STPA.

Losses

Traditional safety is typically focused on loss of life or injury to persons, as well as damage to equipment. However, STAMP-based methods can be widely applied to other losses and other values that stakeholders may want to prevent, such as property damage, loss of sensitive information, environmental pollution, or any other unacceptable loss for the stakeholders [3].

System Boundary

Before analyzing any system, is necessary to define what the system is and the appropriate boundary for the system. A system is defined as a set of components that act together as a

whole to achieve some common goal, objective, or end. It may contain subsystems and may also be part of a more extensive system [15]. Hence, “system” is a practical abstraction defined by the analyst to facilitate and focus the analysis. When analyzing a system, it is important to understand where the system is located and how it interacts with its environment and other systems.

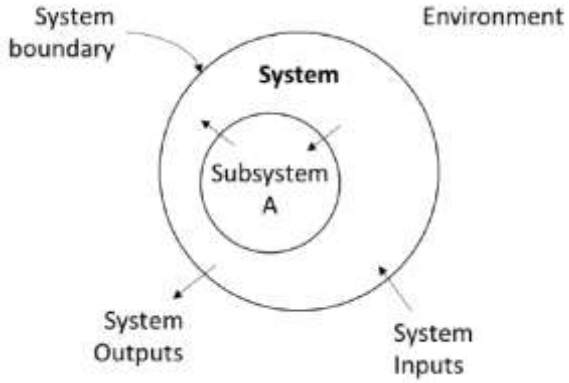


Figure 9: Relationship between system, subsystems and environment [15]

Hierarchical safety control structure

STAMP is based on system theory and views systems in terms of hierarchical structures. Each level in the hierarchical structure imposes constraints on the level below it, and control processes between levels of the hierarchy enforce the safety constraints. An accident occurs when the safety constraints are not adequately enforced by the overall system structure.

The following figure represents how these interactions between levels occur:

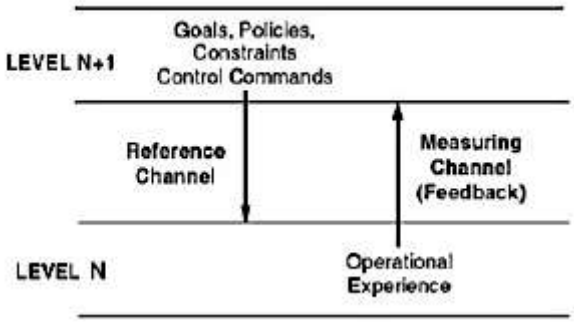


Figure 10: Interactions between different control levels [3]

A generic hierarchical control structure is shown below. Each level provides control actions to enforce constraints on the levels below, and each level may receive feedback from the levels below.

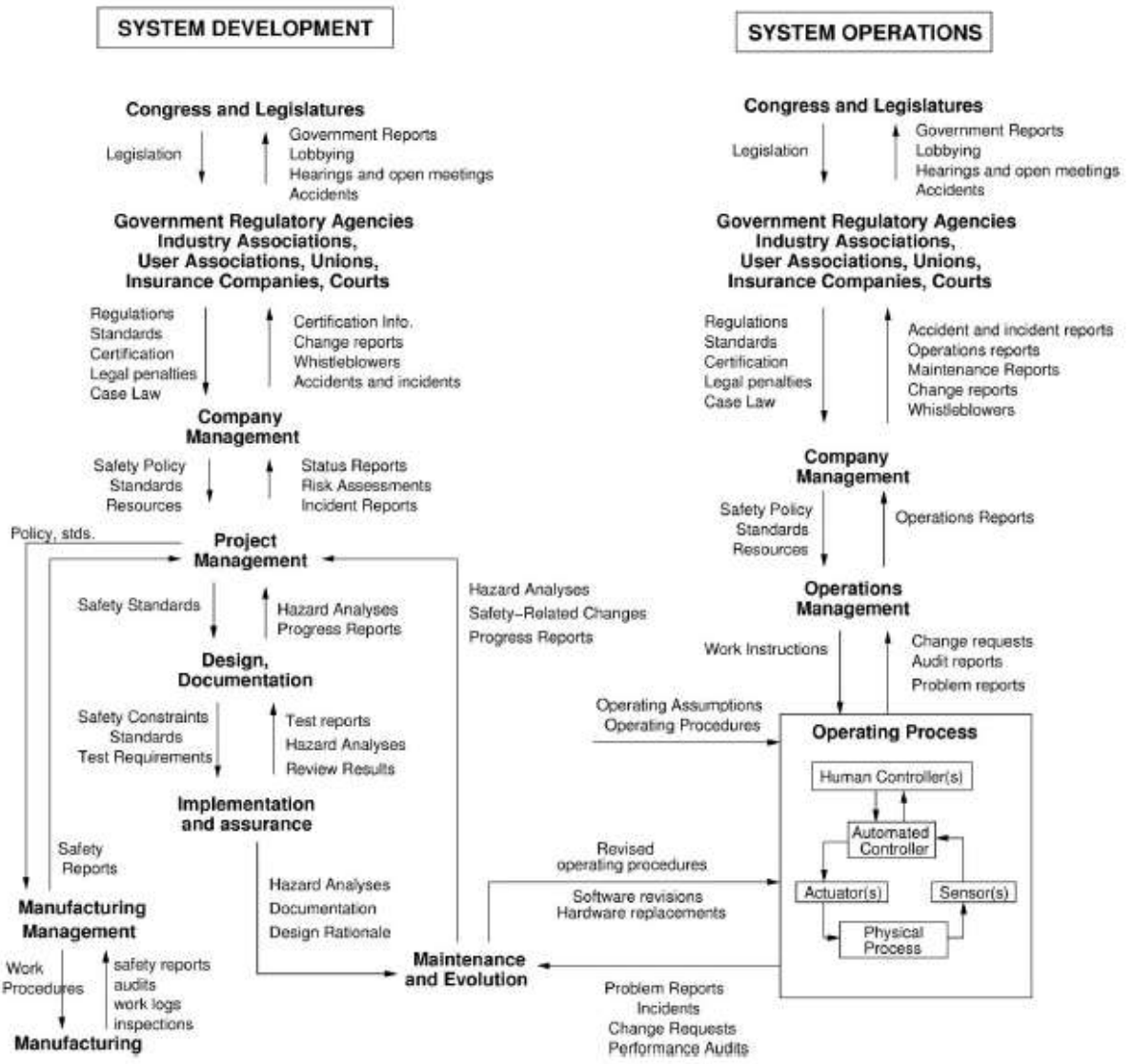


Figure 11: Generic example of a hierarchical control structure [3]

Control loops and process models

Process models are an essential part of control theory. There are four conditions required to control a process. First is the goal. Second, the controller must have appropriate actions to achieve the goal. Third is the observability condition, represented as a feedback channel in the figure below. Finally, there is a model condition, which states that controller must have an internal model or belief representing the current state of the system, the ways the process can modify its state, and relationship between the system variables. The following figure represents how these interactions occur between these elements:

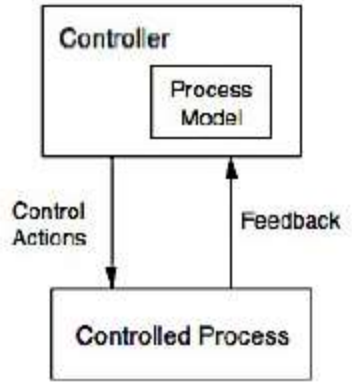


Figure 12: Representation of process models [3]

Flaws and deficiencies in each of these conditions can lead to accident. For example, in STAMP, there are four ways that control actions can lead to an accident [3]:

1. Incorrect or unsafe control command is given.
2. Required control actions (for safety) are not provided.
3. Potentially correct control commands are provided at the wrong time (too early or too late).
4. Control is stopped too soon or applied too long.

These unsafe control actions may be observed not only during operations but also could be anticipated during the design phase to prevent potential mishaps.

3.3.1 CAST: accident analysis

Accidents reports traditionally identify root causes associated with physical sources (equipment failure), contributory causes, and frequently ended assigning the responsibility of the accident to a person. The problem with this approach is the lost opportunity to identify and learn from the full set of system causes that are leading to many different accidents.

The objective in CAST is not to identify single causes alone. Instead, it provides a comprehensive picture of the sociotechnical system by identifying the weaknesses throughout the safety control structure and proposing recommendations to eliminate not only the superficial symptoms but the underlying systemic causes.

Some organizations perform simpler safety analysis because it is easier to blame someone about an accident. However, this approach may be hindering the organization and preventing

identification of the true deeper causes that are behind many more accidents including more catastrophic ones in the future. Unfortunately, complex systems usually are not so simple to have only a single or only a few root causes. Instead, we can minimize biases by using structure methods that identify, for example, why people behaved the way they did given the information they had at the time and the overall structure of the system [3].

In practice, CAST consists of the following steps:

1. Identify the system(s) and hazard(s) involved in the loss.

2. Identify the system safety constraints of each hazard and the system requirements associated with them.

3. Document the safety control structure in place to control the hazard and enforce the safety constraints. This includes the roles and responsibilities of each component in the structure as well as the controls and feedback to execute them.

4. Determine the events leading to the loss.

5. Analyze the loss at the physical level, including:

- Identifying the contribution of physical and operational controls, physical failures, dysfunctional interactions, communication and coordination flaws, and unhandled disturbances.
- Defining why these physical controls were ineffective in preventing the loss.

6. Moving up the levels of the safety control structure, determine how and why each successively higher level allowed or contribute to the inadequate control at the current level.

- Responsibilities related to the prevention of the loss.
- Unsafe or absent control actions.
- Process model flaws.
- Contextual factors and influences on the decision-making process.

7. Examine the overall coordination and communication contributors to the loss.

8. Define the dynamics and changes in the system and safety control structure that led to the loss.

9. Generate recommendations to eliminate or mitigate the unsafe conditions.

3.3.2 STPA: hazard analysis

Systems Theoretic Process Analysis (STPA), is a proactive technique for hazard analysis [15]. STPA was created to address the gaps that are not considered in traditional hazard analysis techniques such as HAZOP.

STPA is a step-by-step process that can be used at any stage of the system life cycle. STPA starts by defining the system of interest and the losses and hazards the system should not cause. The second step is to create a model of the safety control structure. This control structure represents a functional abstraction showing the hierarchy of control between different elements of the system.

The next step is to examine how the control actions could lead to the losses and hazards initially defined. These unsafe control actions (UCA) can be used to create precise requirements and constraints for the system. The UCAs are typically documented in a table that shows the context and conditions under which the control actions are hazardous. The table typically includes one column for each of the four ways a control action could be unsafe

- A control action required for safety is not provided
- An unsafe control action is provided
- A potentially safe control action is provided too early or too late, that is, at the wrong time or in the wrong sequence
- A control action required for safety is stopped to soon or applied too long (for continuous, actions, not discrete ones)

The following table is an example of this representation:

Table 2: Example of a UCA table

Control Action	Not providing causes hazards	Providing causes hazards	Wrong timing /Order causes hazard	Stopped too soon or applied too long
Close Water Valve	Not hazardous	UCA-2: Computer provides close water valve command while catalyst open	UCA-3: Computer provides close water valve command before catalyst closes	Not applicable
Open Water Valve	UCA-1: Computer does not provide open water valve command when catalyst open	Not hazardous	UCA-4: Computer provides open water valve command more than X seconds after catalyst open	UCA-5: Computer stops providing open water valve command too soon when catalyst open

The UCAs should include the conditions in which the action is unsafe. For example, the UCA-1 specifies the condition “when catalyst open”, which is what makes the control action unsafe.

Once the unsafe control actions are identified, scenarios are created to identify how the unsafe control actions could occur and to identify how control actions might not be properly executed or followed. The identification of potential scenarios is vital to understand broader causes and contexts that lead to UCAs and to prevent future events that might not be considered during the design phase or operations.

3.4 Summary of literature review. Comparison between models

The following tables aim to summarize the positive and negative aspects of the accident causality models, as well as the hazard techniques addressed in this document.

This list is not exhaustive, but it serves as a collection of insights to easily distinguish the main benefits and shortcomings of the models.

Accident Models

Table 3: Comparison between accident models

Model	Advantages	Disadvantages
Domino	Easy to apply and to interpret. Does not require significant expertise to apply it	Causality of events are assumed to have a linear relationship. Does not consider the interactions between elements and external factors
	Focuses on workplace safety as it highlights the physical constraints required to enforce safety (e.g. safety guards)	Focus on human error as the cause of all accidents. It promotes the enforcement of methods of control (e.g. procedures, supervision) to avoid human failures instead of systemic factors
Swiss Cheese	The concept is easy to understand. Does not require significant expertise to apply it	Oversimplifies the dynamic of accidents. Does not consider the complex interactions affecting multiple layers simultaneously
	Goes beyond operator actions, including certain organizational factors	Undefined and ambiguous starting point of the analysis that could be defined according to organization bias or convenience
		Does not provide a detailed approach to understand and prevent accidents in complex sociotechnical systems (no method)

Accident Analysis Methods

Table 4: Comparison between accident analysis techniques

Model	Advantages	Disadvantages
Root Cause Analysis	Graphical representation of accident causality	Does not always lead to a root cause identification when the cause is unknown
	Easy to understand the cause-effect relationship	The analysis could lead to disparate sources or possible causes
	Aims to uncover the root causes through the decomposition of causal factors	Requires expertise to identify meaningful causes for the event
		Undefined and ambiguous starting point of the analysis that could be defined accordingly to organization convenience
CAST	Systemic approach to identify causes not only focusing on physical and human causes, but also design flaws, contextual factors, mental models.	Requires some expertise to identify the safety dynamics of the system
	Realize safety as control process where constraints need to be enforced	Sophisticated model for events that have a straightforward causality

	Appropriate to understand safety dynamics of complex systems	

Hazard Analysis Methods

Table 5: Comparison between hazard analysis techniques

Model	Advantages	Disadvantages
HAZOP	Highly structured and systemic examination	Lack of assessing hazards involving the interactions between the elements of the system.
	Widely used in the industry. Applicable to numerous cases	The use of guidewords could miss some potential causes
	Software available to facilitate the analysis	It underestimates the effects of the context on the dynamics of the system.
	Requires a multidisciplinary team (multiple viewpoints)	Time consuming
	Good traceability, easy to document	Expertise and discipline diversity are crucial to the quality and completeness of a study
Bow Tie	The cause-effect link is easy to understand and follow	Lack of framework to define causes and consequences
	Its diagrammatic structure facilitates the analysis. Good for communication purposes	Do not focus on interdependencies, which could be relevant in complex system
	Widely used in the industry	It underestimates the effects of the context on the dynamics of the system
	Software available to facilitate the analysis	Requires expertise to identify the safety dynamics of the system
STPA	Helpful to understand the safety dynamics of complex sociotechnical systems	Time consuming
	It could be use in early stages to identify system requirements and constraints	Requires some expertise to identify the safety dynamics of the system
	Realize safety as control process where constraints need to be enforced	The use of guidewords could missed some potential causes
	Good traceability, easy to document	
	Software available to facilitate the analysis	

Chapter 4: A case study in the steel industry

This chapter is comprised initially by a description of the steel making process, giving a brief technical background to understand the mechanics of an incident that will be the subject of a case study in this thesis. Subsequently, a description of the incident at the company is presented, followed by the Root Cause Analysis performed by the organization to describe the causality of the incident.

After having presented the background of the incident, a CAST analysis is performed to identify with a systemic approach the causes that led to this event. A contrast between the analysis performed by the organization using traditional safety models and the analysis based on STAMP will be presented in the following chapter.

4.1 Steel Making Overview

Since its origins, the steel making process has been a staple of the industrial economy.

The industry has been in constant evolution in the last decades trying to improve its productivity while increasing its safety performance and environmental footprint. Nowadays, two main ways to produce steel exists, through blast furnaces or by electric arc furnaces (EAF). Both technologies have advantages and disadvantages, depending on the accessibility to raw materials, logistics, the cost-structure, and the scoping of the organization, companies decide which option makes more sense to its business plan.

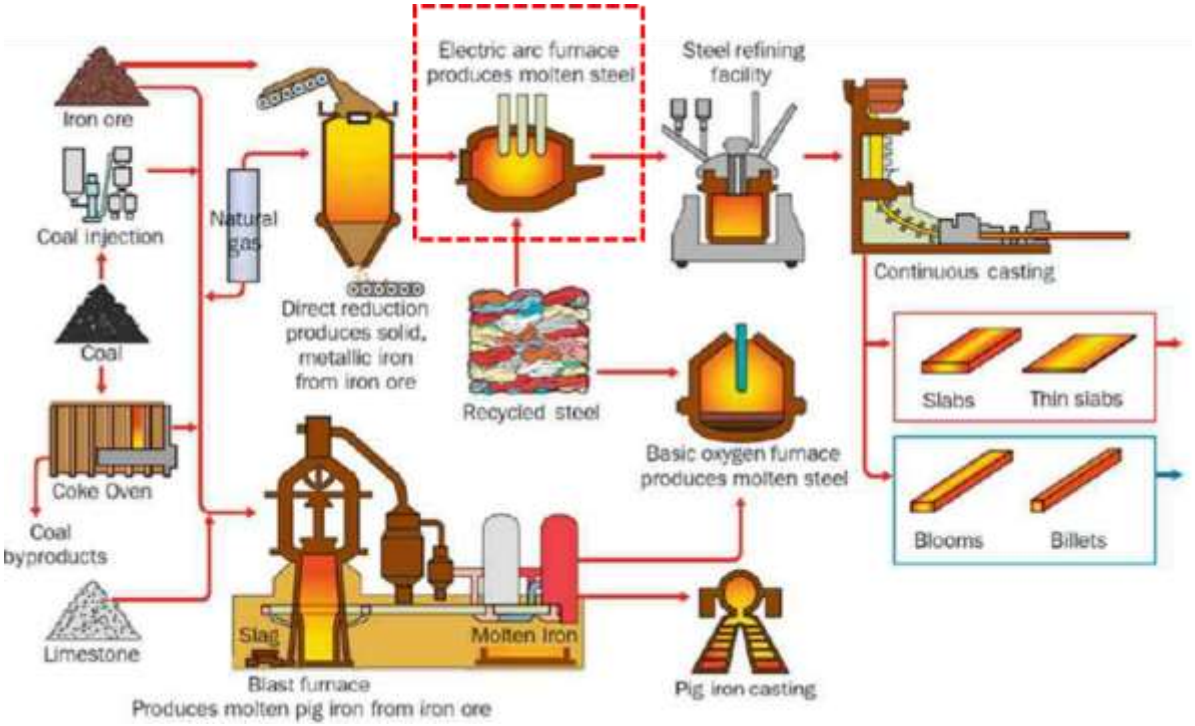


Figure 13: Steelmaking flow sheet [16]. The encircled process corresponds to the electric arc furnace

In the plant where the case study incident occurred, the company operates two EAF. They are identified by their original manufacturer name: Fuchs furnace and Danieli furnace. The incident occurred in the Fuchs furnace; however, the process fundamentals of both furnaces are equivalent, and the following general description is valid for both.

Electric Arc Furnace Construction

The electric arc furnaces are truncated cylindrical vessels with inner walls lined with refractory, and they are covered by a removable roof through which a graphite electrode enters to the inside of the furnace. The EAF is integrated mainly by three sections:

- The shell, which refers to the sidewalls of the furnace and is typically cooled by water.
- The hearth, which consists of the lining refractory inside the furnace.
- The roof, which is a retractable lid in the form of a vault, covered on the inside by refractory and cooled by water. The roof has a center cavity allowing the electrode to enter the furnace to create the electric arc.

The furnaces are separated from the ground floor to provide free space for the ladles and slag pots in the bottom part of the furnaces.

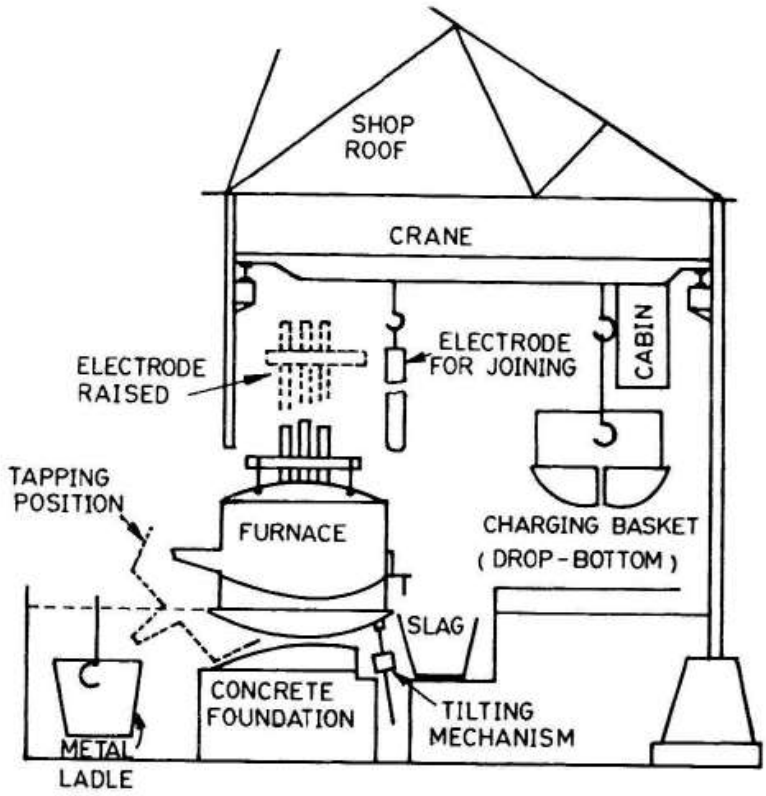


Figure 14: Vertical section of EAF shop [16]

The electrodes and its positioning system are located apart from the furnace structure. Electrodes are the main heating element used in the EAF. They are rounded bars typically made of graphite; this element is selected due to its high conductivity and resistance to high temperatures. The electrodes are attached to a controlled mast which moves the electrode down into the furnace or up out of the furnace. The electric arc is formed between the charged material inside the furnace and the electrodes; the charge is heated by the current passing through the electrodes and the emergent radiant energy. The electric arc temperature could reach 3000°C; hence, the lower section of the electrode glows incandescently during operations, which makes it very difficult to visually distinguish the bottom of the electrode from the molten steel in the furnace and the distance between the two. Therefore, the electrode positioning system has a length encoder to measure the electrode position, and it has hydraulic cylinders to ensure the position of the electrode inside of the furnace maintains a constant current during the melting process [17].

The furnace is built over a basculating structure to be able to pour the molten steel to a ladle to transport it to further processes. This process is called tapping. Most EAF used to produce flat products have an eccentric bottom tap-hole (EBT) to reduce the inclusion of nitrogen and slag in the molten steel, as well reduce the temperature loss of the bath during tapping. In

contrast, the Fuchs furnace has bottom oval-shaped; thus, it has an oval bottom tapping (OBT).

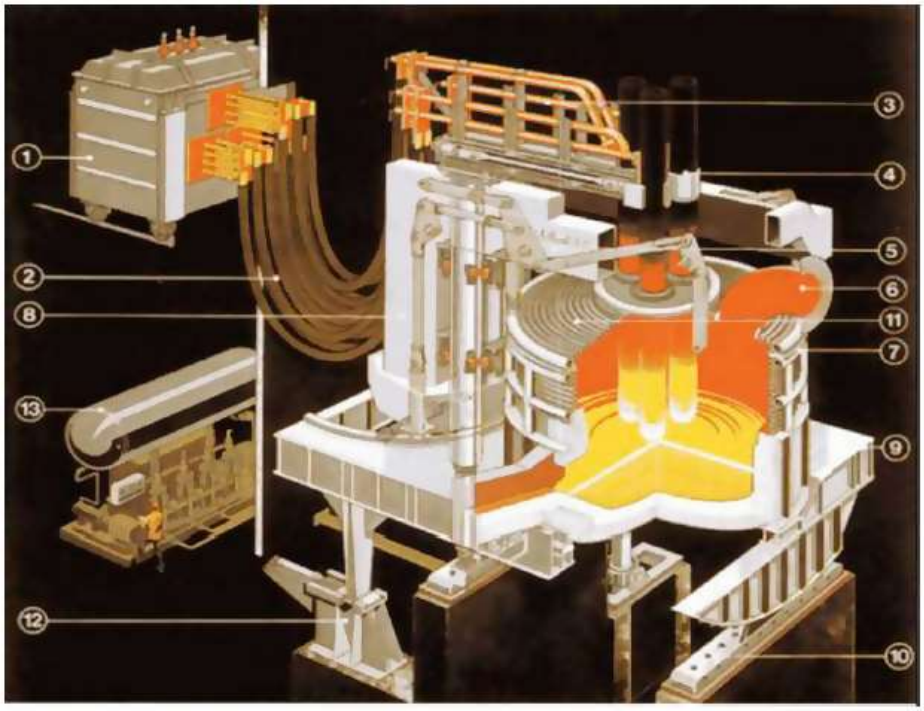


Figure 15: Current EAF standard design [16]

(1) Transformer, (2) flexible cable connection, (3) electrode arms, (4) electrodes clamping, (5) arms, (6) cooled off-gas duct, (7) cooled panels, (8) structure, (9) basculating structure, (10) rack, (11) cooled roof, (12) basculating device, and (13) hydraulic group .

The tap-hole crosses the hearth and shell of the furnace to get to the molten steel. They are closed from outside the bottom steel plate by a refractory sliding gate; when the sliding gate is pulled apart, the metal flows out removing the refractory sand put in earlier to close the hole.

The upper side walls of the shell and the roof of the Fuchs furnace are cooled by water-cooled panels. This mechanism was used to improve the furnace capacity ratio instead of using refractory. These panels are made up of segments and are distributed along the perimeter of the upper shell and the roof.

The Fuch EAF at Guerrero Plant has oxygen-fuel burners in the sidewalls to improve the melting rate and to make the heating of steel more uniform. They provide additional chemical energy by injecting oxygen and carbon into the furnace. The set of injectors are located above the melting bath to avoid damages during the operation.

Physical inspection of the furnace components is vital during and after operations. The traditional refractory linings are made of elements extremely susceptible to water; hence, water leaks need to be treated as critical. In the worst-case scenario, severe refractory

damage could lead to breakouts, where the liquid metal penetrates the refractory and the furnace shell, spilling the steel out of the furnace.

Dedicated maintenance for monitoring and inspecting the physical conditions of the water-cooled panels is critical to avoid safety events. The contact of water and molten steel could cause steam explosions, which are violent reactions due to vaporization of water at extreme speeds, increasing its volume dramatically. These events could cause severe losses and must be prevented.



Figure 16: Example of water panels and their distribution over the sidewalls and the roof of a furnace [16]

Electric Arc Furnace Operation

The operation of an EAF varies depending on the characteristics and specifications of the facility. In the case of the Fuchs EAF at Guerrero plant, the furnace could be loaded with scrap along with direct reduced iron (DRI) for chemical balance.

The scrap is loaded into a large basket with a gate in its bottom. The electrode, which is clamped to the mast, is extracted from the inside of the furnace by the control room operator. Once the electrode is in its upper position, the roof of the furnace along with the electrode swing off the body to facilitate the charging of scrap from the top. To avoid a collision, the electrode needs to be in its top position before the roof starts to move. The electrode swings off through the arm, which is a rotating holder that supports the set of the mast and electrode. The basket is moved by an overhead crane and held just above the furnace. Then the basket opens and drops out the scrap into the furnace. This process is repeated as many times as necessary according to the capacity of the furnace and the baskets.

After the charging is over, the roof is swung back to the operation position. The electrodes are lowered into the furnace, the arc is struck, and the electrodes are set in automatic control. The meltdown starts at a lower voltage to protect the roof and the walls from excessive heat from the arc. The electrode moves down automatically as the metal below the arc melts to maintain a stable arc. Once the electrodes have submerged in the molten steel, and are covered by the

scrap, the voltage is increased, and the electrodes are raised to expand the arc and increase the power to melt. The oxygen-fuel injectors of the Fuchs also provide chemical energy to accelerate the meltdown process [17].

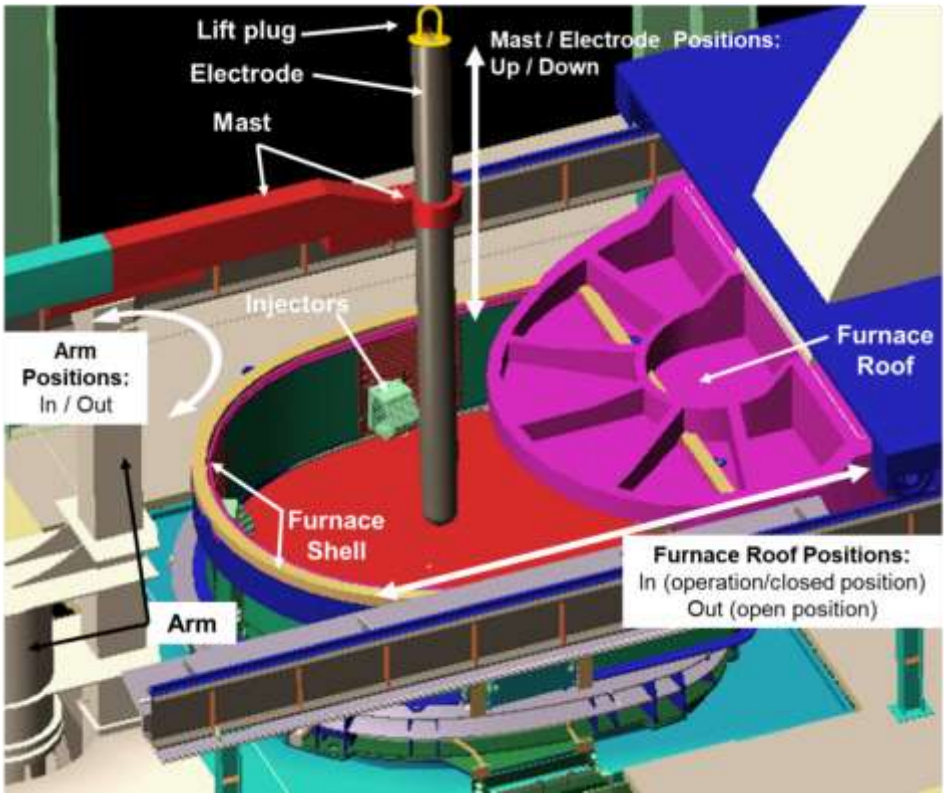


Figure 17: Electric Arc Furnace Operation

The electrodes are consumable elements that need to be replaced after a determined number of charges. To perform this operation, the control room operator extracts the electrode from the furnace interior by raising the mast to its maximum position. The control room operator informs the crane operator that the electrode has reached its top position, and that it is ready to be hooked. The crane operator hooks onto the electrode's lift plug (which is a handing tool screwed to the top of the electrode), and the control room operator releases the mast clamp. Once the electrode is released from the mast, the crane operator raises the crane to remove the electrode from the mast, and moves it to the changing column to replace it. After the worn electrode has been removed, the new electrode is moved and installed in the furnace's mast assembly to continue operations.

During the meltdown, process slag is formed. The slag is made by metal oxides, and acts as a thermal blanket for the molten bath and helps to reduce the erosion and damage of the refractory lining of side walls and the roof. At the end of the melting, the refining process starts to control the impurities and ensures the chemical composition and temperature of the molten bath.

Once the temperature and the chemical composition are adequate, the furnace tilts to tap out the molten steel into a ladle. Typically, some molten steel is left in the furnace to create a hot heel, which helps the following charges to improve the efficiency of the meltdown process. After this process, the furnace is inspected to detect damages in the refractory lining, leaks in cooling panels, and the condition of the electrodes. Once the tapping process ends, the tap-hole is filled with refractory sand.

4.2 Case Study Incident

On October 2nd, 2017 at 11:13 am in the Fuchs furnace at the Guerrero Plant in Monterrey, México, two explosive reactions occurred without hurting any workers, but with enough strength to have caused severe damage to the personnel.

The plant was preparing to restart operations after an extensive maintenance shutdown of 10 days, where significant equipment and systems modifications were conducted. After the refractory sintering process of the furnace, which is a necessary step to develop good properties of the inner refractory bricks, the operations team wanted to extract the electrode from the furnace to check the furnace interior and to replace the electrode. Hence, the main control room operator moved up the mast to take out the electrode from the inside of the furnace. However, the mast did not reach its top position; the control room operator noticed this situation from the encoder indication in one of the HMIs, and he decided to slightly move it down to restart the upward movement again.

By this time, the crane operator had already hooked the electrode onto the lift plug. As the electrode was hooked to the crane at a fixed position, and the mast moved it down, the electrode’s lift plug broke, fell and hit one of the water piping connections over the furnace roof.

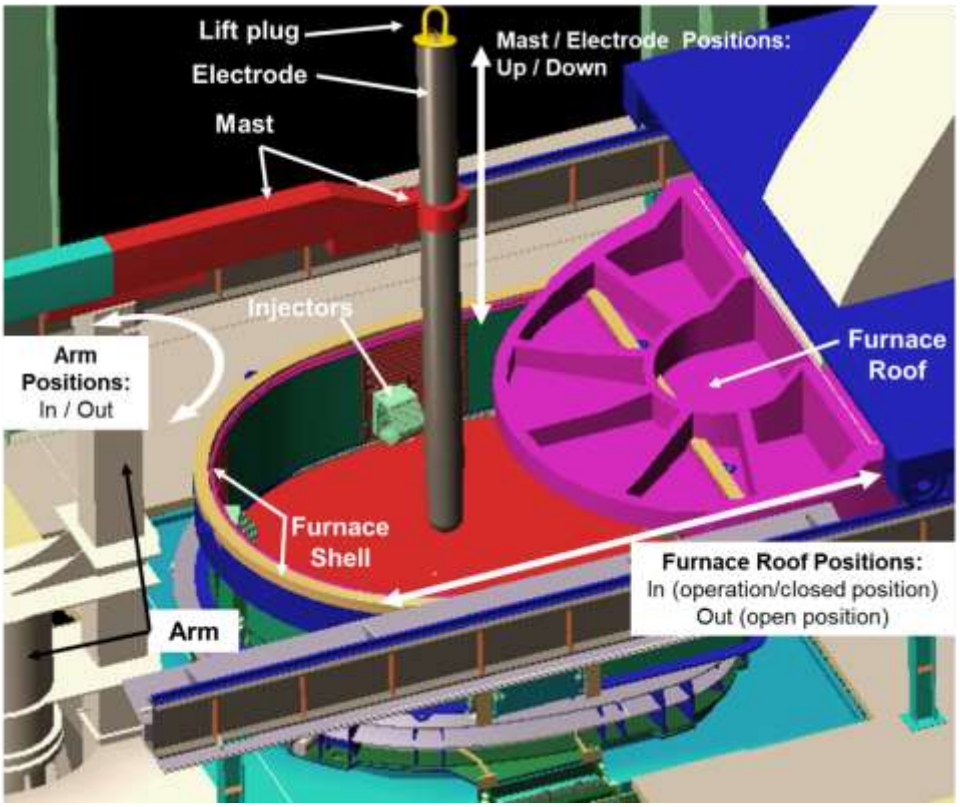


Figure 18: Fuchs electric arc furnace

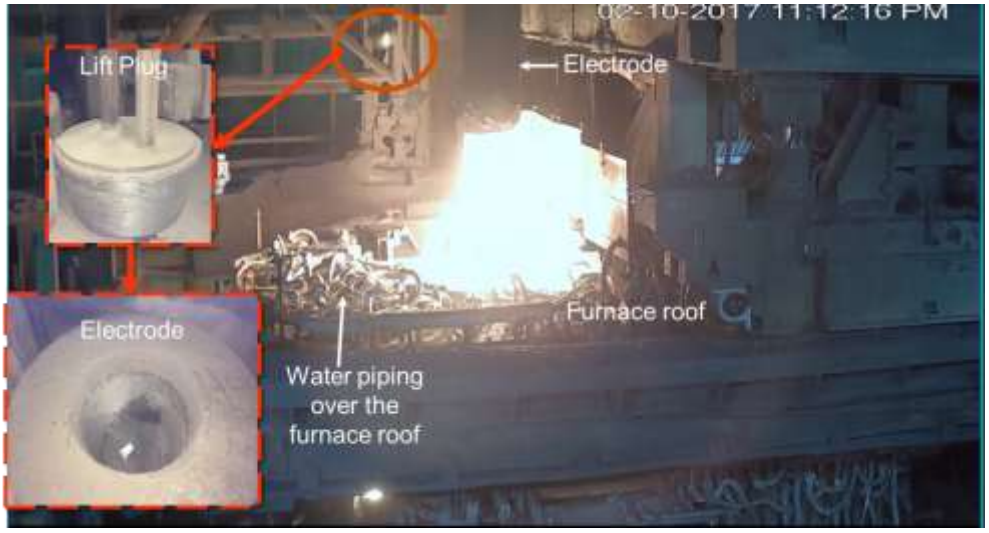


Figure 19: The moment when the electrode's lift plug broke

This impact caused a severe water leak that was getting into the furnace. As a reference, the lift plug weighted 85 kg (187 lbs), and the piping connection had a diameter of 2 inches and 4.5 bar of pressure.

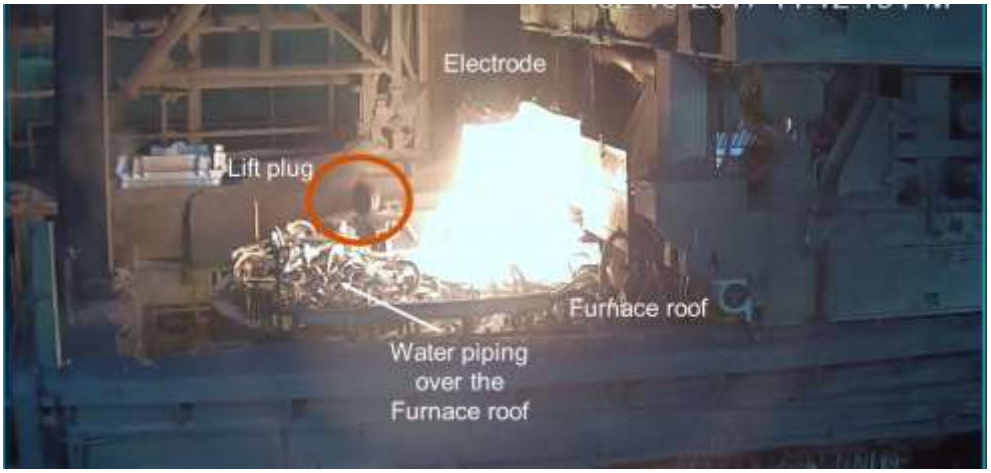


Figure 20: The lift plug fell towards the water piping over the furnace roof

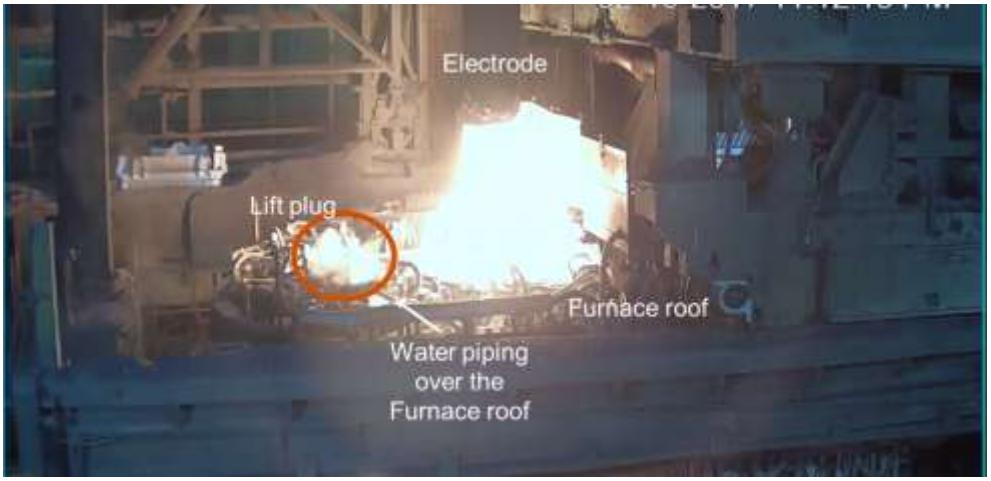


Figure 21: The lift plug hit the water piping over the furnace roof

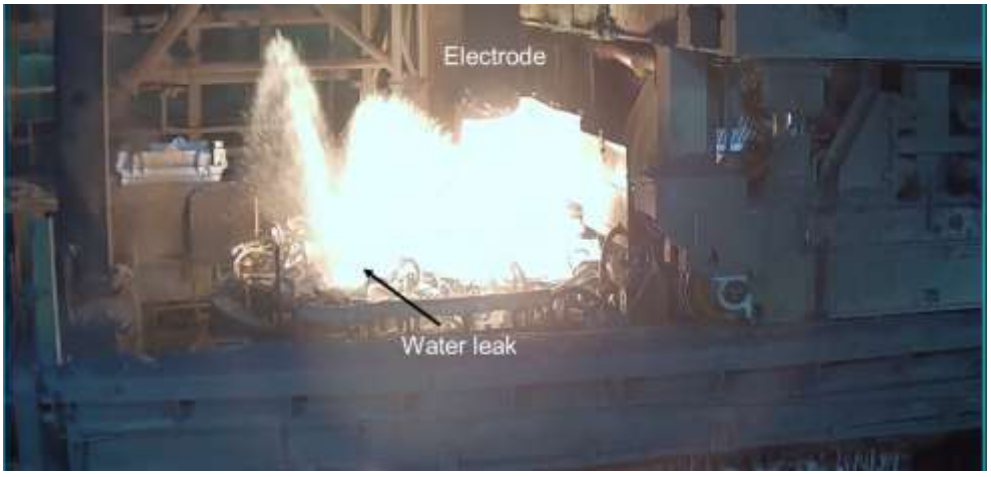


Figure 22: Water leak due to the damage of water piping

According to safety procedures, since the water was getting inside of the furnace, the furnace roof had to be open. The control room operator started the sequence to move out the roof from its operating position to its open position; however, as the electrode did not reach its top position and it was below the pass line of the furnace roof, the roof collided with it. The control system, which was designed with various safety protections to prevent dangerous movements, allowed the movement of the furnace roof even though the electrode had not been raised enough to prevent a collision. The electrode fractured due to the collision, and one segment of it fell inside the furnace, causing an explosive reaction.

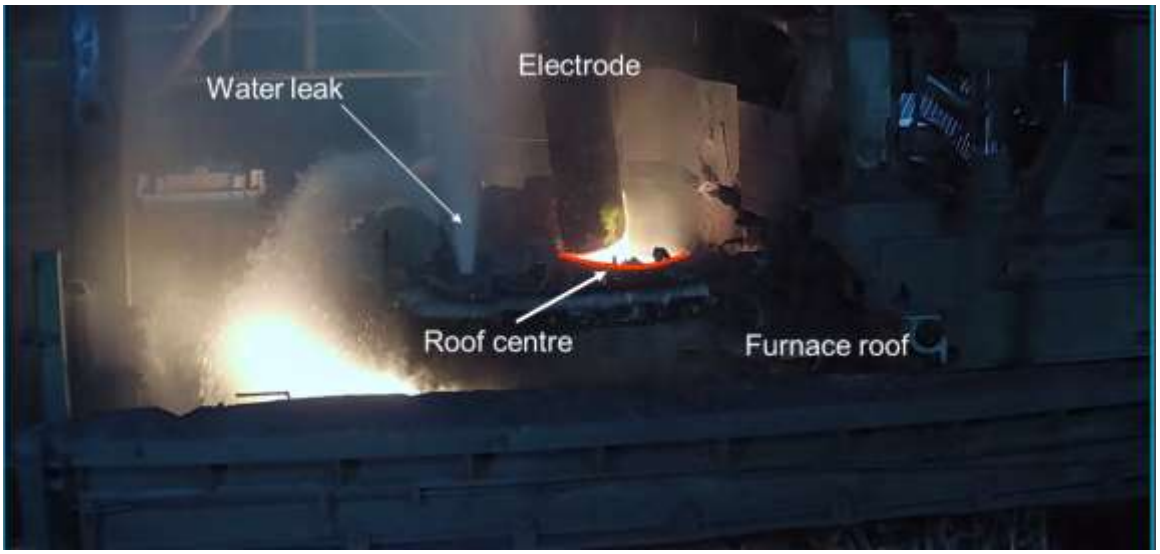


Figure 23: Electrode is damaged by the furnace roof while opening it

During this time, the water leak continued to get into the furnace. Because of the trajectory of the water leak, as the furnace roof continued to open it allowed even more water to enter into the furnace. The electrode segment that fell inside of the furnace caused agitation of the molten steel; this agitation, coupled with the water accumulation, generated a second explosive reaction.

During the event, the emergency protocol was performed and all people were evacuated. The operations team shut down the furnace and closed the injections of gas, coal, and oxygen. The maintenance team closed the cooling system valves. Despite the severity of the event, no people were injured.

The previous description reflects what is stated in the company's internal report. However, a good accident analysis method should raise new questions and potentially uncover more information about additional causes that have not been uncovered. Discovering additional causes that have previously gone overlooked is important because it leads to a broader set of

potential solutions that can be considered and used to prevent future incidents and accidents. These broader solutions may be more effective, less expensive, and may prevent more types of accidents than only focusing on a narrow set of obvious causes. The Root Cause Analysis in section 4.3 and the CAST analysis in section 4.4 will explain any addition questions that were raised and present any additional causes and potential solutions that were produced. These analysis methods will then be compared in Chapter 5.

4.3 Root Cause Analysis performed by the company

The company performed the following Root Cause Analysis of the incident previously described. Traditionally in the organization, the leader of the analysis is the manager where the accident occurred. In this case, as the incident occurred during the restart of operations, the operations manager led the analysis with the support of the safety team and the participation of the engineering and maintenance management team.

The analysis is divided into two sections: the first part considers the first reaction after the damage in the water piping of the furnace roof and the subsequent falling of the electrode segment into the furnace.

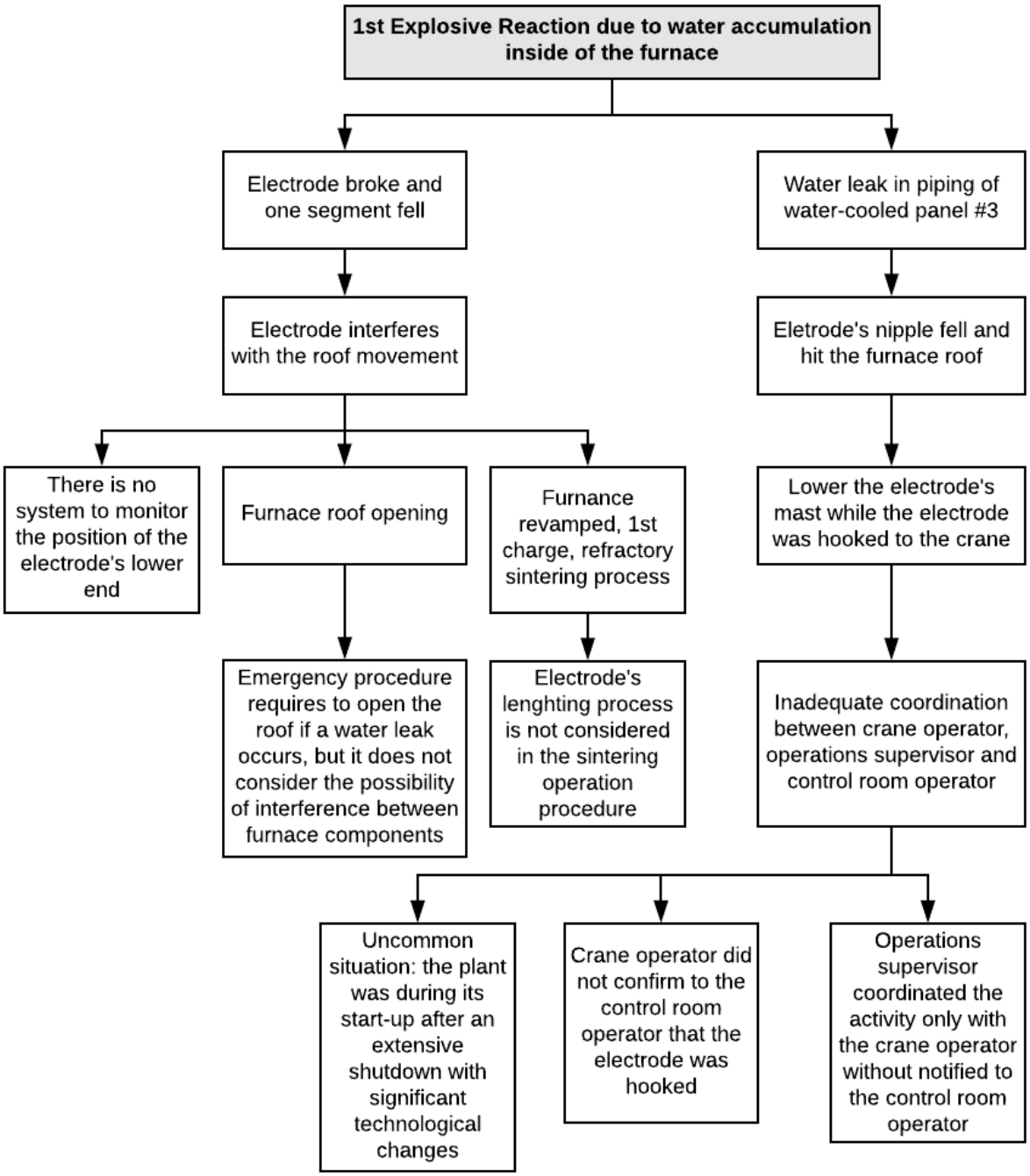


Figure 24: Root cause analysis of the first reaction performed by the company

The analysis has two branches, one related to the leak in the cooling system (right branch), and other for the electrode's rupture (left branch). Two separate causality branches suggests both events were considered distinct with no strong correlation.

The sequence of events shown on the right of the Figure 25 explains the dynamics that might have led to the fracture of the electrode's lift plug which hit the water piping on the furnace roof producing a severe water leak. The sequence implies that a primary cause of this event was the inadequate coordination between the crane operator, the supervisor, and the main control

room operator. This poor coordination entailed the lack of confirmation from the crane operator that the electrode was already hooked to the crane, and missing communication between the control room operator and the operations supervisor.

On the left side of the diagram, the sequence of events suggests the rupture of the electrode was related to an inadequate monitoring due to the lack of an appropriate system to determine the electrode's position. The electrode's position was determined only by a length encoder. Before the modification of the main control room, the operators used to have a visual reference in the front window of the control room; while this reference was archaic, it was a method that operators felt comfortable with using to verify the position.

The analysis affirms that the standard procedure to swing the furnace roof in case of a water leak did not consider the possibility of a contact between the electrode and the roof. By this, the analysis suggests the necessity to have protections to avoid a collision between the roof and the electrode.

The second section of the analysis aims to describe the mechanics of the second reaction due to the water accumulation inside the furnace.

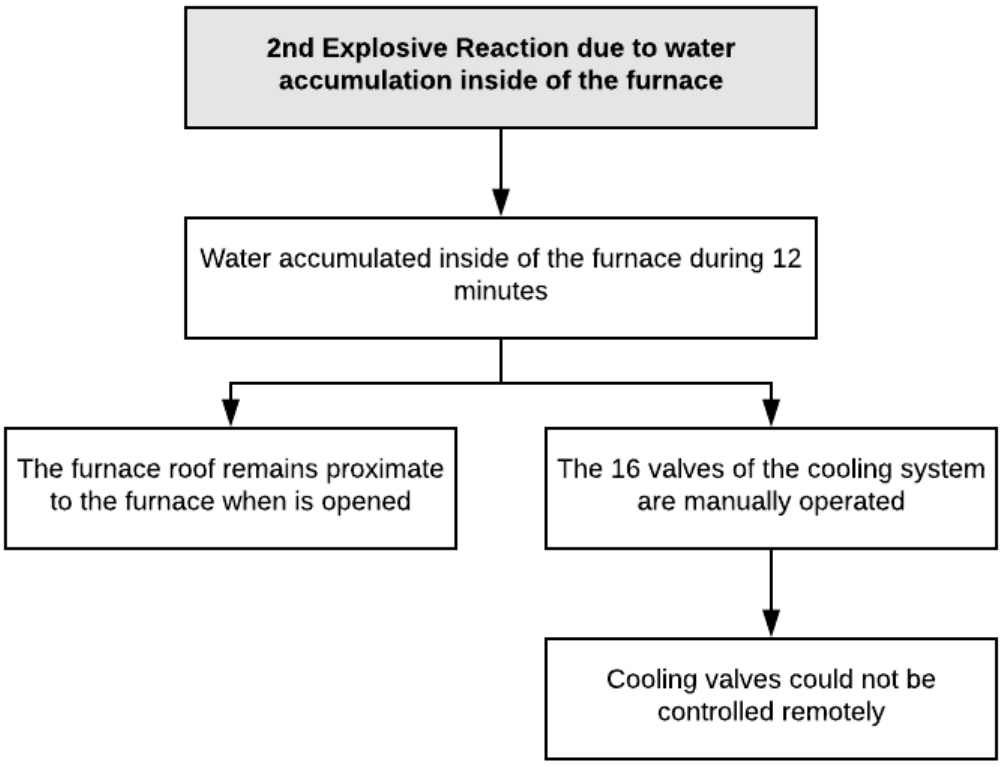


Figure 25: Root cause of the second reaction performed by the company

The analysis of the second reaction indicates the water accumulated inside of the furnace for twelve minutes, and this was due to the lack of valves that could be controlled remotely. As the sixteen cooling valves needed to be handled manually, the time to close them was too long.

The other cause referred to in the analysis is related to the proximity of the roof to the furnace while it is open. As the vicinity of the roof was close to the furnace, the water coming from the leak in the roof went directly inside the furnace, rapidly increasing the accumulation of water.

After having defined the causality branches, the company identified a list of causes and grouped them into three causality clusters:

Physical Causes

- The main control room was moved during the shutdown to a safer position. However, the visual reference the operators used to validate the electrode position was lost after this change.
- The valves of the cooling system were not possible to operate from the control room. The valves were manual; hence, the reaction time to close them was significant.
- The position of the roof while opened remained proximate to the furnace, causing the water to rapidly accumulate inside the furnace.

Systemic Causes (Management system):

- During the tapping sequence, the electrode did not reach its top position at 649cm; it raised only to 618cm.
- The control room operator lowered the electrode mast 30 cm since he noticed it did not reach its top position. He lowered the mast trying to enable the automatic control.
- The control system was weak because the control room operator could activate the roof-swing sequence while the electrode was not in its top position and not clear of the roof.
- It was an atypical operation since the plant was during its start-up process after an extensive shutdown with several technological changes.

Human Causes:

- Inadequate communication between the crane operator, operations supervisor, and the control room operator.

The methodology followed by the company identified these three causality clusters, and the causes related to them. It is interesting to notice that all the identified systemic causes described in the analysis do not correspond properly to systemic factors. The causes, as described in the analysis, should be classified as physical causes since they are related to equipment failures or control flaws. It may be that the way they were phrased does not reflect fairly the intention to address a systemic cause. However, it is notable that the report did not identify systemic causes of the event.

Additionally, the causality report does not review other relevant factors involved like the disabled protections of the control system during start-up or why they were disabled. Another factor that does not appear in the analysis is the organizational acceptance of the deficiencies in the electrode's position system and how it became an acceptable practice to perform startup with recognized faults in the system [18].

Although the severity of this incident resulted in additional effort and scrutiny during the root cause analysis, indirect factors and decisions made long before an incident tend to be overlooked by traditional root cause analysis methods. For example, prior to this incident the piping connections in the furnace roof had been changed to facilitate its future maintenance, making them more exposed to damage as they were above the level of the roof protection beams. The maintenance team did not consider the possibility of falling heavy objects that could damage the piping in the hazard analysis that was performed and therefore little protection from falling objects was included in the design. The modification that exposed piping connections in the furnace roof was not correctly documented, suggesting that the management of change process was also inadequate and making it difficult to perform a proper hazard analysis. However, none of these factors appear in the root cause analysis that was performed. There is a clear need for an analysis method that can systematically raise questions, identify overlooked system vulnerabilities, and identify both direct and indirect causes that can be addressed to prevent future incidents and accidents.

The next section applies a different analysis method called CAST. This method was designed to help understand the whole picture of an incident by not only focusing on the physical causes alone but also understanding the context and mental models underlying the event. The objective of CAST is not to assign blame or to identify only direct and proximate causes, but to systematically raise new questions that may not have been explored previously and to understand what safety constraints may be missing throughout the technical, human, and organizational structures involved.

4.4 CAST Analysis

4.4.1 Identify the system

In this case study, the system is comprised of the Fuchs EAF including its roof, the electrode positioning system (mast, arm, and electrode), and the furnace cooling system. Support equipment such as the furnace crane and all the organization involved in the steel making process is also part of the system, along with the safety standards, procedures and regulations.

4.4.2 Identify the losses, hazards and safety constraints

The losses associated with the incident are:

L-1: Loss of life or injury to people

L-2: Loss of or damage to equipment

L-3: Loss of customer satisfaction

The first loss refers to the damage that the incident may cause directly to the people working nearby the facility. The second refers to the damage to the equipment itself and the surrounding equipment. The last one is related to the impact on fulfilling clients orders due to the lack of production capacity.

The hazards and safety constraints associated with the incident are listed below. The relationships between the losses and the hazards are identified with brackets.

H-1: Furnace integrity is lost [L-1, L-2, L-3].

The safety control structure must ensure:

- **SC-1:** Furnace must be design so that integrity is assured under worst-case conditions.
- **SC-2:** Furnace must be adequately monitored to detect abnormal operations that threaten furnace integrity and measures must be taken to prevent the loss of integrity.

H-2: Furnace unable to be cooled [L1, L2, L-3].

The safety control structure must ensure:

- **SC-3:** Cooling must be provided and adequate to maintain process within a given temperature range
- **SC-4**: Any inability to provide cooling must be detected and emergency actions taken to control the process immediately

H-3: Furnace is physically damaged during operations [L2, L-3].

The safety control structure must ensure:

- **SC-4:** Operations that would damage the furnace must be prevented

H-4: Furnace releases or projects dangerous material to surroundings [L1, L2].

The safety control structure must ensure:

- **SC-5:** Dangerous material must not be released or projected when workers are close to the furnace.
- **SC-6:** Evacuation alarms must be available all times and must operate under the worst circumstances when there is a danger to workers

4.4.3 Safety control structure

A simplified high-level control structure of the incident at the Guerrero Plant is provided in the next figure. This structure shows the system at a high level of abstraction. Since the incident was an internal safety event without more significant consequences (e.g. worker's injuries, damages to the community), no government or regulatory entities are shown in this diagram.

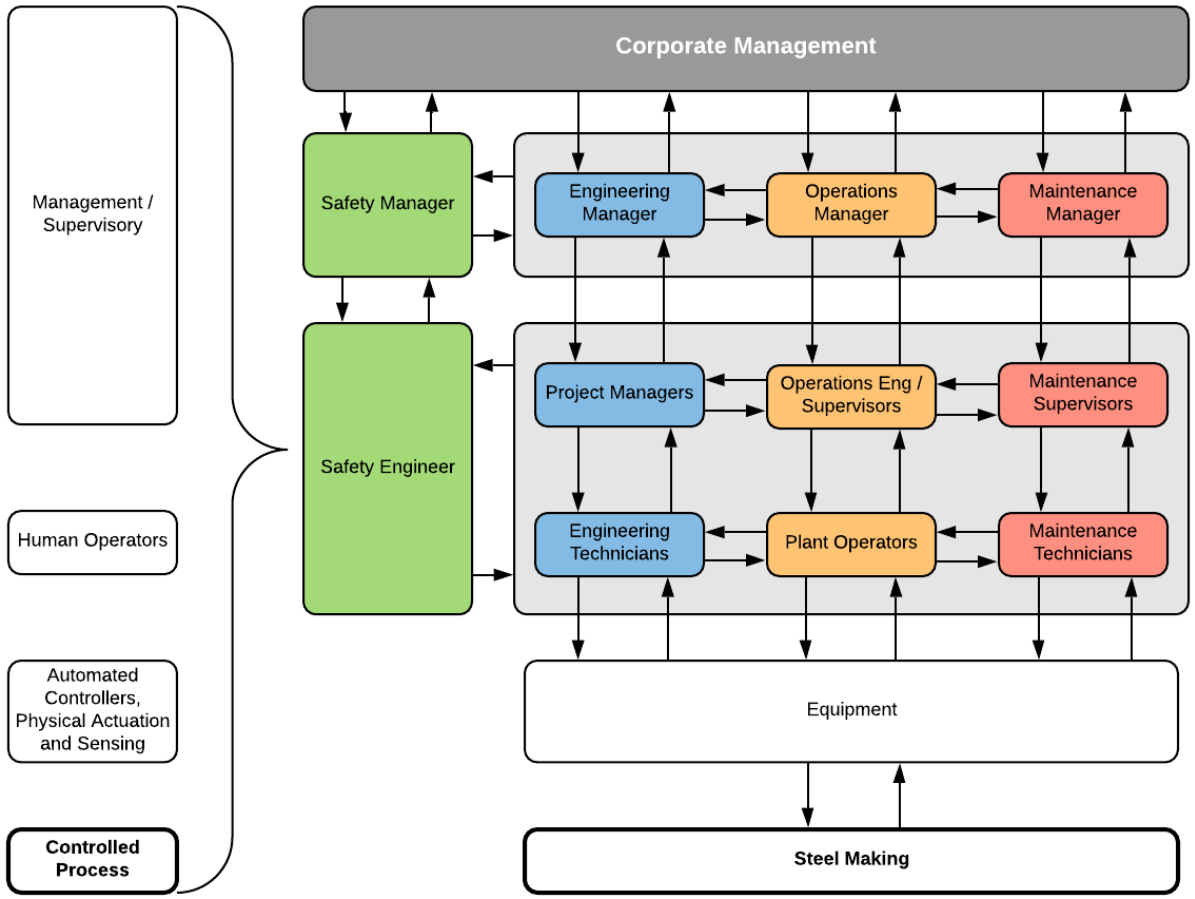


Figure 26: Level 1 high-level safety control structure

Figure 27 shows the level 1 safety control structure related to the event. This control structure is focused on the different management branches within the company who had a significant role in the accident and its outcome. It explicitly shows the safety team as an independent staff area providing support to the rest of the management branches; this interaction is represented as a gray area encompassing the engineering, operations, and maintenance teams. This is a simplified structure that manifests only the relevant actors in this safety event, so it does not include all the aspects of the company or its operation.

It is important to note that the objective of this analysis is to find the safety weaknesses in the system to identify opportunities to improve, and not to blame the people involved. Hence, the safety control structure used in this analysis is based on roles and not specific individuals.

Figure 28 depicts the level 2 safety control structure as a zoomed-in version of the high-level control structure. In this representation, the teams are broken down into specific elements, and the interactions between them are illustrated. The diagram starts at a level of plant workers and goes upward to the corporate management of the company. It shows in more

detail the management and supervisory structure, as well the human controllers (workers, operators, technicians), the controller (equipment), and the controlled process (steel making).

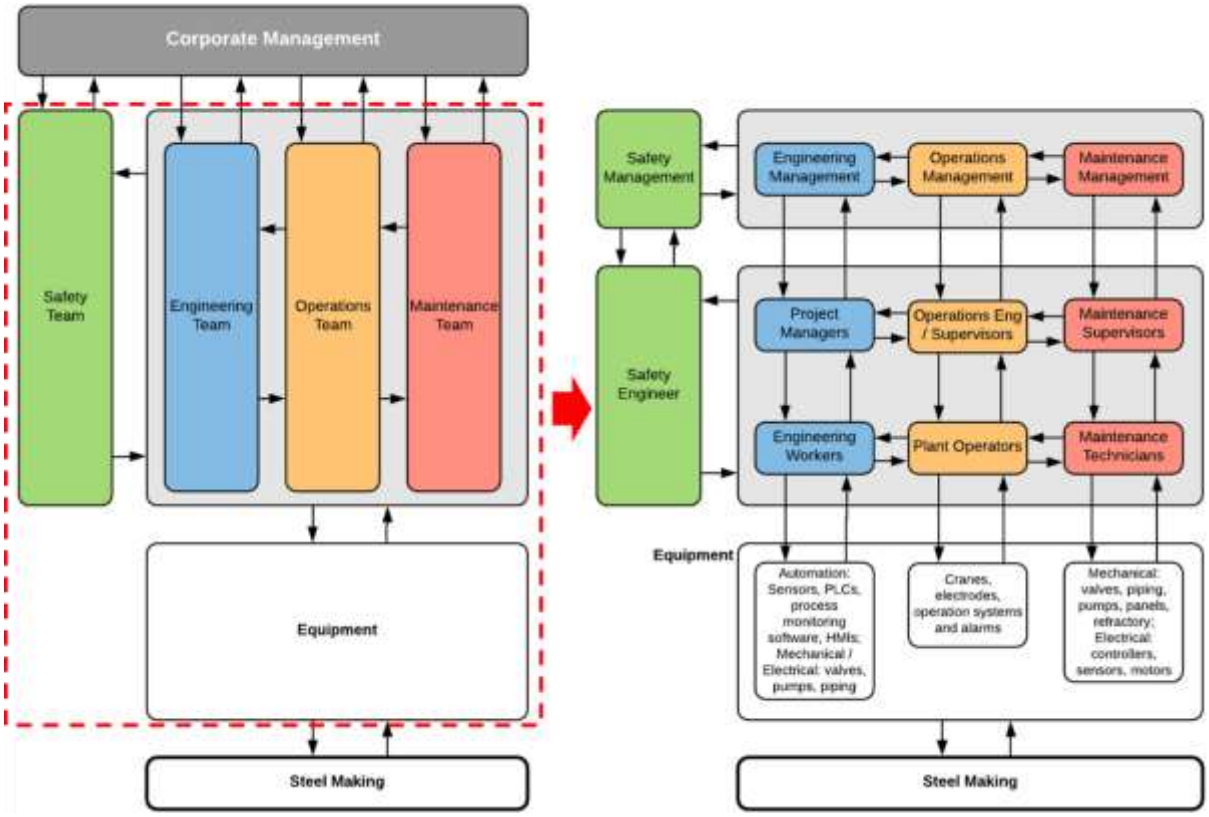


Figure 27: Level 2 high-level safety control structure

These management branches can be analyzed as subsystems of the control structure:

- **Safety Team**: refers to the team responsible for the safety management system. It is integrated into two elements:

    - Safety manager: who is responsible for establishing policies and procedures to promote the health and safety of every person inside the company's facilities and ensure their compliance with applicable standards and regulations. Safety managers are fundamental as they are the guardians to ensure safety rules as the prevalence principles in all company operations.

    - Safety engineers: they are responsible for monitoring the compliance of safety standards at the floor level. Their role is critical as they have more experience and a more trained eye to identify hazards; therefore, they serve both as guidance and auditor to preserve the integrity of the workers. Safety engineers are encouraged to understand the processes to identify where are the main risks; at the same time,

they need to be close to the workforce to understand their concerns and have insights about what is happening at the floor.

The safety team provides guidance and support to the rest of operational areas to perform hazard assessments and non-routine work authorizations to assess the hazards of and to control work in other than normal operations (e.g., start-ups, shutdowns).

- **Engineering Team**: refers to the area responsible for designing, building and implementing new technologies or to revamping current processes by replacing obsolete or old technologies according to operations and maintenance requirements. All these activities need to follow safety and environmental standards and regulations. It is integrated into three elements:

  - Engineering management: responsible for delivering projects on time and budget, according to user requirements in compliance to safety standard and regulations. The engineering management, according to user needs, defines the prioritization of projects and the allocation of resources to face them. The projects are subjected to an evaluation to determine if they have a reasonable economic return; if that was not the case, as many safety-related projects, they need to be justified as critical for safety purposes. The project portfolio needs to be approved firstly by the corporate management.

  - Project manager: responsible for the design and implementation of projects. They are the primary liaison between the users and the engineering team; they have to have a clear picture of what the needs and requirements from the users are, as well as understand the project context. All these inputs are essential to identify the hazards related to the project, and to perform the assessments to control and mitigate them.

  - Engineering workers: this element refers to the engineers and technicians participating in the project. They are supervised by the project manager and have tight coordination with the operations and maintenance team. They have to understand the relevance of the project, the requirements, its constraints, and hazards to ensure a successful project implementation.

The engineering team had a strong relevance in this incident since it occurred after an extensive shutdown where significant engineering changes in some equipment took place; particularly, some of these changes were related to the relocation and revamping of the main control room, upgrade of process controls, and the redesign of all human-machine interfaces. These elements had a profound impact on the way to operate and maintain the plant.

The following diagram shows a more detailed safety control structure for the engineering team.

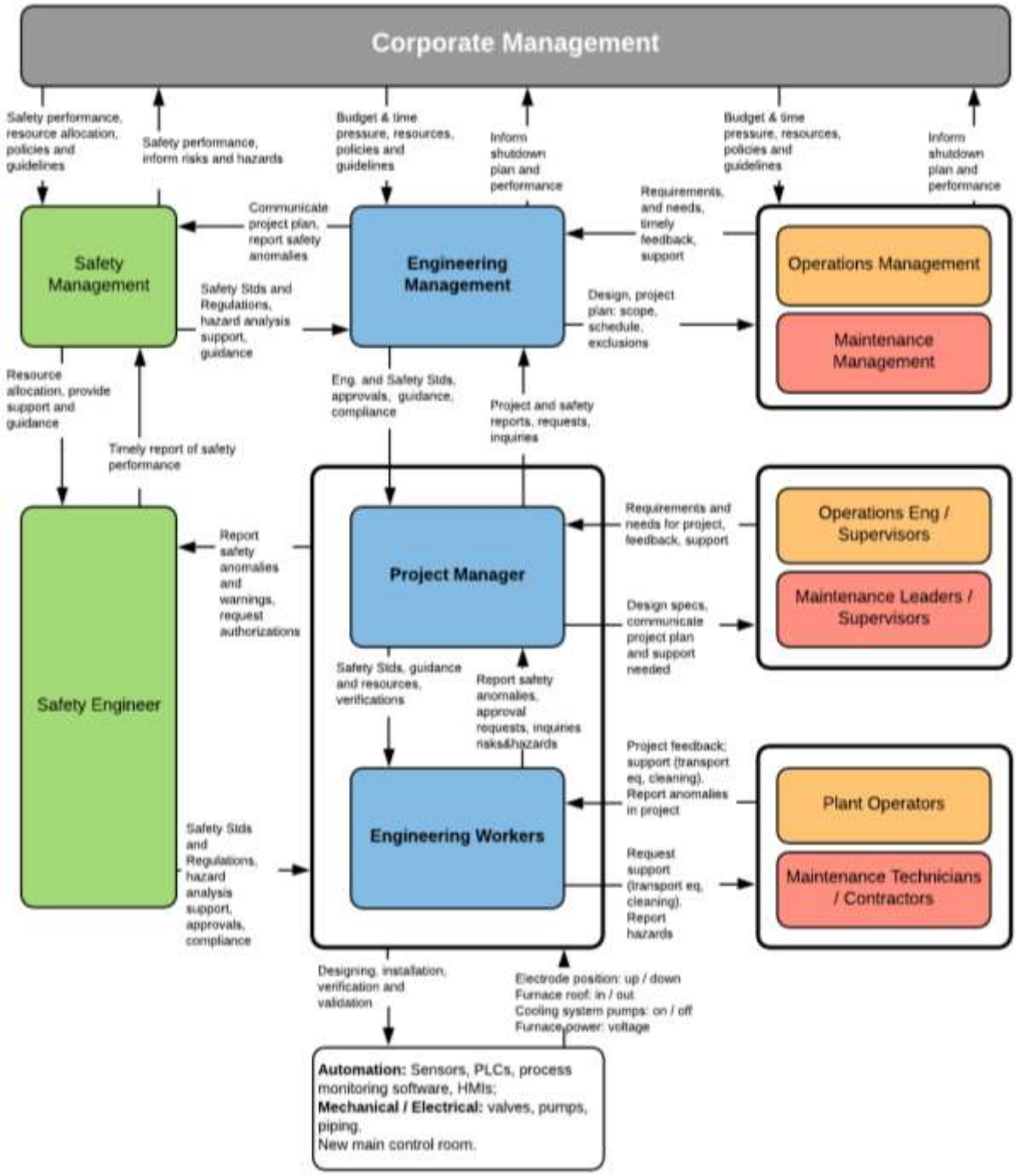


Figure 28: Detailed engineering safety control structure

This diagram provides insight into the interactions between the engineering team and the rest of the management branches and system elements. It is important to note that the interactions of the operations and maintenance hierarchy are not shown in this diagram since it is only focused on the engineering organization and its relationship with other structures. Later in this document, the interactions between operations and maintenance will be detailed.

Due to size constraints, a full description of all interactions could not be included in these diagrams; they provide only an overview about the interactions between the elements. A detailed description of the information exchange between elements can be found in Appendix 1 and 4.

In addition to engineering, it is also important to understand operations and maintenance:

- **Operations Team**: refers to the area responsible for operating, monitoring, and controlling the steel making process. Like the previous branches, it is composed mainly of three elements:

    - Operations management: responsible for plant operations. In charge of defining the standard procedures to operate with safety and ensuring their compliance. This element comprises some actual positions in the organizational hierarchy: the head of operations, and the operations manager. This abstraction was considered for simplification purposes since both positions shared similar responsibilities regarding safety management.

    - Operations engineers and supervisors: key elements accountable for safety and operations at the plant floor during the event. One of the critical responsibilities of the operation supervisor was to ensure that the activities performed by the elements of the system complied with the safety procedures and standards defined by the organization. They played an active role in safety management.

    - Plant operators: this element concern to the workers performing activities at the floor or in control rooms. Their leading role was to perform their activities according to safety and operation procedures defined, as well as reporting and control any anomalies while performing their duties.

The operations team activities are fundamental for safety management, and particularly in this event since the plant was restarting operations after a major shutdown. Operations also

provides support to maintenance and engineering teams to perform their activities during the shutdown.

- **Maintenance Team**: this element refers to the team responsible for maintaining the equipment integrity to achieve minimum breakdowns in compliance with safety procedures and standards. Similar to the previous branches, it was composed mainly of four elements:

    - Maintenance management: responsible for defining and ensuring the compliance of maintenance procedures and safety standards. Like operation management, this abstraction comprises the heads of mechanical maintenance and electrical maintenance. It also includes the maintenance manager. They share similar safety responsibilities, and they promote that the performance of maintenance tasks is under the core principles of safety within the organization.

    - Maintenance leaders and supervisors: like the operations engineers and supervisors, the maintenance leaders and supervisors were crucial elements accountable for safety and maintenance tasks at the plant during the event. The primary role of the leaders and supervisors is to ensure that activities are performed according to procedures and safety standards. They monitor the activities, and guide inquiries or requests from the technicians or contractors. They are also responsible for authorizing the work permits to perform the planned maintenance tasks. During major shutdowns, they have to closely supervise the activities performed by contractors to ensure their compliance with the company standards.

    - Maintenance technicians: this element refers to the workers performing activities at the floor or in control rooms. Their leading role is to perform their activities according to the defined safety and maintenance procedures, as well as reporting and controlling any anomalies while performing their duties.

    - Maintenance contractors: this element is important since contractors performed many activities during maintenance. They have to perform their activities according to procedures and safety standards defined by the company. This was a challenge for the company since it did not have full control over their technical or safety skills.

A detailed control structure is shown in the next figure to capture the dynamic of interactions of the operations and maintenance teams, and between them and the rest of organization.

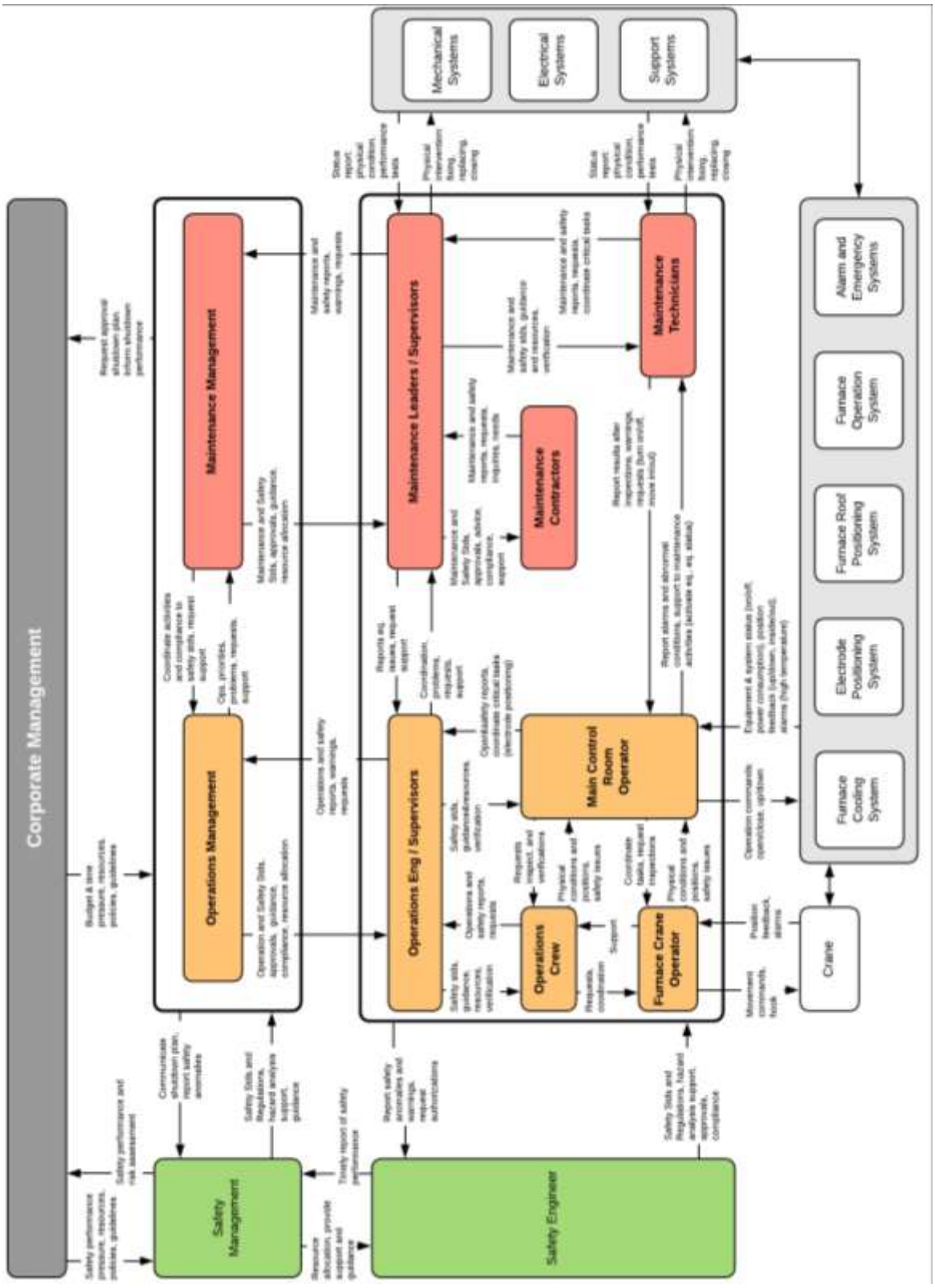


Figure 29: Safety control structure for operations and maintenance

Like Figure 29, this diagram does not include an extensive description of the interactions between elements. That detailed information can be found in Appendix 2 and 3.

Figure 30 specifies the interactions between systems (electrical, mechanical or support) and the maintenance team. The incident occurred during an extensive scheduled maintenance shutdown; thus, several types of equipment were intervened (e.g., fixed, replaced, closed, modified) to improve the performance of the facility.

The diagram specifies the systems (furnace cooling, electrode positioning, furnace roof positioning, furnace operation, alarm, and emergency), and equipment (crane) that were operated by the operations team during the start-up of the plant. The overhead crane, which was used during the positioning of the electrode, was controlled by the crane operator. The main control room operator controlled the rest of the systems through the HMIs located inside of the new control room.

Given the information gathered from the previous control structures, it is possible to summarize the interactions between all elements in a dependency structure matrix. This visual representation summarizes the complex interactions of the system in a concise way to highlight relevant patterns.

The following square matrix shows the interactions between the elements of the system. The “X” inside the cell denotes an interdependency and an exchange of information between elements.

	Eng Tech	PM	Eng Mgmt	Control Room Oper	Oper Crew	Crane Oper	Oper Eng & Sup	Oper Mgmt	Maint Cont	Maint Tech	Maint Lead &Sup	Maint Mgmt	Safety Eng	Safety Mgmt	Corporate Mgmt
Eng Tech		X		X	X	X				X			X		
PM	X		X				X				X		X		
Eng Mgmt		X						X				X		X	X
Control Room Oper	X				X	X	X			X			X		
Oper Crew	X			X		X	X						X		
Crane Oper	X			X	X								X		
Oper Eng & Sup		X		X	X			X			X		X		
Oper Mgmt			X				X					X		X	X
Maint Cont											X		X		
Maint Tech	X			X							X		X		
Maint Lead &Sup		X					X		X	X		X	X		
Maint Mgmt			X					X			X			X	X
Safety Eng	X	X		X	X	X	X		X	X	X			X	
Safety Mgmt			X					X				X	X		X
Corporate Mgmt			X					X				X		X	

Figure 30: DSM of safety control structure

It is evident that the safety management structure, particularly the safety engineer, has several interdependencies across the system. Also, it is appreciable how the medium-level roles, such as the operations engineers and supervisors, and the maintenance leaders and supervisors,

have the most interactions (besides the safety engineer who leads this indicator). This provides an idea of how much the safe control of operations at the plant relied on them.

Additionally, the operations team is the one with the highest concentration of interactions within the system. These takeaways will be revisited later in this thesis.

4.4.4 Proximal events leading to the loss

The next step in CAST is to identify the sequence of proximal events. The following lists the sequence of events leading to the two explosions based on the investigation report from the company safety team. As mentioned before, the plant was about to restart operations when the incident occurred. The furnace was at the end of the refractory sintering process; therefore, the control room operator started the procedure to extract the electrode from the inside of the furnace.

11:10:49	The arm/electrode started to go up.
11:11:09	The arm/electrode stopped at 618 cm (top position was 649 cm).
11:12:05	The arm/electrode retracted to 582 cm (36 cm below previous position).
11:12:16	The lift plug of the electrode broke and fell over the furnace roof.
11:12:17	The lift plug damaged some piping connections over the roof, generating two water leaks: one at 45° towards the outside of the furnace, and another that was directed into the furnace.
11:12:46	The operator started the sequence to open the furnace roof, while the water leak was getting into the furnace. The furnace roof started rising.
11:13:21	Finished furnace roof rising.
11:13:30	Started furnace roof opening (swinging).
11:13:34	The furnace roof crashed and damaged the electrode while swinging. The electrode broke, and one segment fell inside the furnace.
11:13:35	The electrode segment hit the molten steel, and the first reaction occurred.
11:21:35	The water leak started to decrease.
11:26:47	Water stream at 45°stopped.
11:32:10	Second reaction occurred due to accumulated water inside the furnace.

4.4.5 Analysis of the loss at a physical system level

This section studies the physical and operational controls at the system that contributed to the event.

Physical safety requirements and constraints related to the incident:

- PSR-1: Prevent explosive reactions in the furnace. [H-1, H-4].
- PSR-2: Warn operators when the cooling system is operating close or below its safety threshold. [H-2].
- PSR-3: Prevent water from entering and accumulating in the furnace. [H-3]
- PSR-4: Prevent collision between movable elements of the furnace. [H-3].
- PSR-5: Activate the siren in case of emergency. [H-4].
- PSR-6: Provide adequate protection against human exposure to the reaction. [H-4].

Physical controls and equipment to enforce the requirements above:

- PCE-1: Instruments (sensors) to monitor the cooling system. [PSR-1, PSR-2, PSR-3].
- PCE-2: Equipment (e.g. valves) to control the cooling system on timely manner. [PSR-3].
- PCE-3: Emergency stop to halt furnace operation. [PSR-1].
- PCE-4: Vacuum to capture water vapor from the furnace. [PSR-3].
- PCE-5: Furnace roof to prevent water from entering into the furnace. [PSR-3].
- PCE-6: Protection shield over the piping of the roof furnace. [PSR-3].
- PCE-7: PLC to control the position of the furnace components (e.g. roof, electrode) [PSR-4].
- PCE-8: Sensors (e.g. linear encoders) to monitor the position of furnace components. [PSR-4].
- PCE-9: Alerts on HMIs to notify the risk of collision due to physical interference between furnace components. [PSR-4].
- PCE-10: Audible emergency evacuation signal. [PSR-5].
- PCE-11: Restricted areas to avoid having people close to the furnace. [PSR-6].
- PCE-12: Protective equipment for employees. [PSR-6].

Failures and inadequate controls in the physical equipment:

- FIC-1: The operators were unable to monitor the status of the cooling system. [PCE-1].
- FIC-2: The operators were unable to shut down the cooling system in case of an emergency. [PC-2].
- FIC-3: The piping over the furnace roof was damaged by a fallen object. The damage caused the water leak. [PCE-6].
- FIC-4: The position of the roof while opened remained close to the furnace, causing the water leak to get quickly into the furnace. [PCE-5].
- FIC-5: The PLC did not avoid the collision between furnace components (e.g. roof and electrode). [PCE-7].
- FIC-6: The mast failed to reach its top position when the operator extracted the electrode from the furnace's inside. [PCE-8].
- FIC-7: The operator did not receive an alert on the HMI about the potential collision between the roof and the electrode when he moved the roof to its open position. [PCE-9].
- FIC-8: The operator did not have adequate feedback to determine the precise position of the lower part of the electrode. [PCE-7].
- FIC-9: The audible evacuation signal did not sound when the operator tried to activate it. [PCE-10].

Contextual factors that explain the physical failures or inadequate controls:

- CF-1: The cooling system did not have sensors to monitor its status. In the case of pressure drops or leaks, the operators could not detect these conditions. [FIC-1].
- CF-2: The cooling system valves were manually operated. The control room operator could not control them. Closing the valves was an activity that could last hours. The maintenance team performed this task. [FIC-2].
- CF-3: During the shutdown the maintenance team increased the length of the piping to make it easy to maintain, as the space to handle was constrained in the previous design. The length increase of the piping made it more vulnerable to be damaged by fallen objects. [FIC-3].
- CF-4: The PLC to control the position of the furnace components was replaced during the shutdown because it was saturated and obsolete. The former PLC used to have protections to avoid collision between the movable components of the furnace. However, during the startup, the protections on the new PLC were disabled. Thus, the

furnace roof was able to move even though the electrode was interfering. [FIC-5, FIC-7].

- CF-5: During the maneuver to take out the electrode from inside the furnace, the control room operator detected that the electrode did not reach its top position. This was not the first time this failure occurred. The operators had reported the failure, but the management decided to not intervene the PLC that controlled the furnace component positions due to its critical condition, and because it was going to be replace soon during the shutdown. So, the operators developed a non-standardized practice to deal with the issue. [FIC-6].
- CF-6: The main control room was relocated during the shutdown to put it further away from the furnace for safety reasons. The operators used to have a visual reference (tape on glass) in the front window of the former control room, to help them validate the position of the lower part of the electrode. This verification helped them to check if the roof was cleared to move without interference. However, this reference was lost when the control room was relocated. [FIC-8].
- CF-7: The evacuation emergency siren was disconnected to during the relocation of the main control room. Although, it was not enabled before the plant startup. [FIC-9].

4.4.6 Analysis of the loss at the control system level

Having analyzed the physical system level, the next step is to examine the higher levels to understand why these inadequacies and behaviors occurred. A complete understanding of the event requires an analysis of how and why the safety control structure allowed this to happen. It is crucial to understand the reasons underlying the behaviors and actions of the people involved in the incident. It is helpful to consider the following factors as suggested by Stringfellow [14]: history, resources, tools and interfaces, training, human cognition characteristics, pressures, safety culture, communication, and human physiology.

As previously mentioned, four main management branches were identified: operations, maintenance, engineering, and safety. Each human controller will be analyzed to identify their safety-related responsibilities, unsafe control actions, process model flaws, and context. For traceability purposes, all of them are coded to identify the relationship between them.

Understanding the factors that lead people to act the way they did provides essential insights to make changes and ensure different decisions in the future. The analysis is ordered from the bottom to the upper layers of the organization to explain the broad set of factors that lead to this incident.

Operations Team

The operations team is comprised of the plant operators, the engineers and supervisors, and the management. Plant operators is an abstraction that represents different operational positions, such as the crane operator, the main control room operator, and the rest of operations crew. Similarly, operations management captures the head of operations of the EAFs, and the operations manager.

Table 6: Analysis of loss at the control system level. Plant Operators

Plant Operators (Crane operator, Main control room operator, Operations crew)
Safety Related Responsibilities • **SR-1:** Follow safety procedures and standards while performing their activities. • **SR-2:** Determine, correct, and report operational safety anomalies. • **SR-3:** Prioritize safety as the primary value of the company. No emergency, production process, or results justify putting people's occupational safety or health at risk.
Unsafe decisions and control actions • **UCA-1:** The control room operator moved the electrode down while it was hooked to the crane. [SR-1]. • **UCA-2:** Operators created and followed nonstandard procedures that were inadequate to deal with the electrode's positioning issue. [SR-1, SR-2]. • **UCA-3:** The control room operator swung open the furnace roof while the electrode was below its pass line and not clear of the roof. [SR-1]. • **UCA-4:** The control room operator moved the electrode without having a visual reference to validate its precise position. [SR-2]. • **UCA-5:** Plant operators restarted operations without performing a pre-startup safety review (PSSR) to check operational readiness, including systems, equipment integrity, and organizational factors. [SR-2, SR-3]. • **UCA-6:** Plant operators restarted operations without PLC safety protections in place. [SR-3].
Process Model and Mental Flaws • **PM-1:** The control room operator believed the electrode was not hooked to the crane. [UCA-1].

- **PM-2:** The crane operator believed the operator in the control room knew the electrode was hooked to the crane. [UCA-1].
- **PM-3:** Operators believed the recurrent failure in the electrode's position system could be tolerated and was not a potential cause of accidents. [UCA-2].
- **PM-4:** The control room operator believed the pass line of the furnace roof was clear without interferences. [UCA-3].
- **PM-5:** Operators knew that designed safety protections were not activated, but they believed that it was safe to continue the start-up. [UCA-4, UCA-6].
- **PM-6:** Plant operators believed one of the goals of the start-up was to test the new features of the PLC, so finding inactive safety protections were not unusual. [UCA-6].

Context

- **C-1:** The control room operator and the crane operator coordinate tasks through radiofrequency. The supervisor directly told to the crane operator to hook the electrode without informing the control room operator over the radio. [PM-1, PM-2].
- **C-2:** As the plant was in its start-up process, the communication radio channels were busy, making it hard to understand and follow instructions. [PM-1, PM-2].
- **C-3:** The operators developed a nonstandard practice to deal with the recurrent failures of the electrode's positioning system. Sometimes, when the operators tried to extract the electrode from the furnace, the mast did not reach its top position, stopping a few centimeters below the threshold from detecting maximum position. Thus, the operators slightly lowered the mast, and then manually moved it upward from the HMI to enable the system. This practice turned out to be effective to deal with the issue and become a nonstandard workaround. The operators have previously reported these system deficiencies and the practice that they were using to their superiors. However, the system deficiencies were not corrected. [PM-1].
- **C-4:** The standard procedures were not revised to address the deficiencies of the system that the control room operators uncovered. [PM-1].
- **C-5:** During the plant start-up, several failures in the automatic sequences and protections occurred. For example, one of the protections in the former PLC disabled the movement of the furnace roof if the mast was not at its top position. This protection was not configured in the new PLC used to restart the plant operations. [PM-1, PM-5].
- **C-6:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. While they believed that not having the safety protections

was tolerable, this perception may have shaped by the pressure they were facing due to the shutdown delay. [PM-5, PM-6].

- **C-7:** During the shutdown, the control room was moved to another location (farther away from the furnace). Additionally, all the HMIs were replaced by new standardized interfaces. The visual reference the operators used to have (tape on glass) to determine the position of the electrode was not present in the new location. [PM-4].
- **C-8:** Both the control room operator and the crane operator were relatively new in their positions (less than six months). [UCA-5].
- **C-9:** The pressure to restart production was higher than the pressure to stop production if a non-relevant safety issue was discovered. After shutdowns with major modifications, failures in new equipment, and performance out of standard were acknowledged as part of the business by the organization. Therefore, the failures in automation sequences and protections were considered as normal for a start-up. Thus, the operators continued with the process. [PM-5].

The control room operator extracted the electrode from the inside of the furnace to continue with the furnace inspection. To perform these tasks, the operator pressed the button on the HMI to raise the mast with the electrode. However, like previous occurrences, the electrode did not reach its top position and aborted the automatic sequence. Hence, he performed a nonstandard practice to deal with this repetitive issue. This practice was to briefly move the electrode down to re-enable the automatic control (and ultimately get the electrode into the proper top position). He did not believe the crane operator had hooked the electrode at this time because he never instructed the crane operator to hook the electrode. He believed the crane operator would have notified him if the crane was hooked to the electrode. Additionally, he had no visual or other feedback to indicate the crane had been hooked to the electrode.

Simultaneously, the supervisor directly told the crane operator to hook the electrode without informing the control room operator about it. Also, the crane operator performed this task faster than the normal time it typically required. Therefore, the electrode was already hooked to the crane when the control room operator lowered the electrode. The opposite movements exerted tensile stress over the electrode's lift plug, causing its fracture. The broken lift plug fell and crashed over the water piping of the furnace roof, generating the water leak.

As the broken lift plug hit the piping over the furnace roof, causing a critical water leak that was getting inside the furnace, the control room operator opened the furnace roof as stated in the emergency procedures. The plant manager validated this operation, and the roof was

opened to mitigate the damages of an imminent explosion. Although the electrode was below the pass line of the roof, the management considered preferable to open the furnace although they knew the roof would collide with the electrode.

However, the operators had problems in the past with the electrode's positioning system. As mentioned previously, sometimes the electrode did not reach its top position and instead aborted the automatic sequence to position the electrode at the top. To overcome this situation, the operators developed a nonstandard procedure: they took manual control and moved the electrode down to re-enable the automatic control. This practice was normalized and turned into an acceptable procedure to allow the continuity of operations. The organization was aware of this nonstandard practice and did not take any action to stop it, which reinforced the view among operators that it was an acceptable practice.

Additionally, during the shutdown, the main control room was relocated further away from the furnace for safety purposes. A more modern pulpit with new safety protections such as ballistic windows was installed. However, the organization did not consider that the previous control room used to have a visual reference (a tape on the window) which served as a threshold to validate the physical position of the electrode. Although this verification method was archaic, it proved to be effective for the operators. When the control room was relocated, this reference was lost. The operators were told to operate in the new control room without having this reference, so they had no choice. This reference was relevant for the operators, as they did not have any other mechanism besides the indicator from the linear encoder of the electrode's positioning system.

Table 7: Analysis of loss at the control system level. Operations Engineers and Supervisors

Operations Engineers and Supervisors
Safety Related Responsibilities • **SR-1:** Follow safety procedures and standards while performing their activities. • **SR-2:** Determine, correct, and report operational safety anomalies. • **SR-3:** Prioritize safety as the primary value of the company. No emergency, production process or results justify putting people's occupational safety or health at risk. • **SR-4:** Develop operating procedures to control the hazards adequately. • **SR-5:** Oversee operations to ensure the (safety-related) policies and procedures are being followed. • **SR-6:** Provide training to operation team on plant hazards and safe operating procedures. Audit to see if training has been effective.

- **SR-7:** Promote adequate safety behaviors through an evident commitment to safety to prevent accidents and incidents.
- **SR-8:** Ensure safe delivery of equipment conditions before shutdowns; additionally, ensure a safe start-up after maintenance shutdowns.
- **SR-9:** Generate a suitable Safety Emergency Plan and ensure its compliance.

Unsafe decisions and control actions

- **UCA-1:** The supervisor requested the crane operator to hook the electrode without informing the control room operator. [SR-1].
- **UCA-2:** Did not request the operators to perform a pre-startup safety review (PSSR) to check operational readiness, including systems, equipment integrity, and organizational factors. [SR-2, SR-3, SR-8].
- **UCA-3:** Approved to restart production without safety protections in place. [SR-3, SR-8].
- **UCA-4** Did not assess potential risks associated with substandard and nonstandard operations and did not provide corrective actions. For example, the nonstandard procedure used to deal with the electrode's positioning issue. This practice was not revised and properly documented. [SR-3, SR-5].
- **UCA-5:** Did not assess potential shortcomings related with the changes in the plant (e.g., the loss of visual reference to validate the electrode's position due to the relocation of the main control room, or the modification of the piping length over the furnace roof). [SR-8].
- **UCA-6:** Developed safety procedures inadequately detailed to manage an emergency due to a severe water leak. [SR-4].

Process Model and Mental Flaws

- **PM-1:** The supervisor believed the control room operator had noticed that the crane operator hooked the electrode. [UCA-1].
- **PM-2:** The supervisor believed the mast stopped because it reached its maximum position or at least reached a sufficient height to continue the operation. [UCA-1].
- **PM-3:** The supervisor may have believed that since the mast had stopped, the control room operator had stopped the motion and was now waiting for the crane to hook the electrode. [UCA-1].
- **PM-4**: The operations engineers and supervisors may have believed the PSSR was not relevant as the organization did not require it. [UCA-2].
- **PM-5:** The operations engineers and supervisors agreed to continue the plant start-up despite the safety protections in the PLC to control the position of furnace components

were not activated. They believed it was safe to continue the start-up under this condition. [UCA-3].

- **PM-6:** They believed the nonstandard workaround to deal with the failures in the electrode's position system was only a temporary measure and not a potential cause of accidents. [UCA-4].
- **PM-7:** They believed the relocation of the control room would not have impacts in the plant operations. The engineers and supervisors forgot to request an alternative method to verify the position of the electrode since the visual reference would be no longer effective due to the relocation of the control room. Similarly, they believed the modification of the piping length over the furnace roof was an improvement and would not cause safety issues. [UCA-5].
- **PM-8:** The engineers and supervisors believed the procedure that described the process to follow in case of an emergency due to a water leak was good enough to control the emergency. [UCA-6].

Context

- **C-1:** The control room operator and the crane operator coordinated tasks through radiofrequency. The supervisor directly told the crane operator to hook the electrode without informing the control room operator by radio. The crane operator failed to notify the control room operator that the electrode was hooked. [PM-1].
- **C-2:** The PSSR was not a common practice in the organization. A formal procedure did not exist to perform it. The operations team conducted a mental check based on the expertise of the operators, supervisors, and engineers to validate the readiness of the facility to start operations. [PM-4].
- **C-3:** For the organization, having problems during the plant start-up was not an ideal situation, but it was considered part of the process. The supervisors acknowledged it and decided that it was feasible to continue the start-up but demanding more attention and coordination from the operators to ensure ta safety start-up. [PM-5].
- **C-4:** The PLC to control the position of furnace elements was in a critical condition due to its saturation and obsolescence. The engineering team had planned to replace it by a new model during the shutdown. Therefore, while the engineers and supervisors recognized that workarounds were not ideal, the risk to repair the PLC to solve the electrode's positioning problem could be problematic. So, they decided to wait for the replacement of the PLC and considered the nonstandard practice as an effective and safe temporary solution. [PM-6].

- **C-5:** During the shutdown, the control room was moved to another location (farther away of the furnace), and a new standardized interface replaced the previous HMIs. The visual reference the operators used to have (tape on glass) to determine the position of the electrode was lost. [PM-7].
- **C-6:** No similar incidents had occurred in the Fuchs furnace in recent years. Therefore, the engineers and supervisors did not think about different failure scenarios while documenting the procedure to control water leaks. [PM-6].
- **C-7:** The pressure to restart production was higher than the pressure to stop production if a non-relevant safety issue was discovered. After shutdowns with major modifications, failures in new equipment and out-of-standard performance were acknowledged by the organization as normal conditions during a start-up. Therefore, the engineers and supervisors may have assumed that failures could occur during this process, so they requested to operators to be attentive in operation to detect and solve the ongoing anomalies. [PM-5].

During the activity of moving the electrode out of the furnace, incoordination occurred in the operation's team. The control room operator raised the mast, but the control system erroneously stopped before reaching its maximum position. The operations supervisor was at the floor at that moment and had no way of knowing that the control system acted erroneously. He may have believed the mast stopped because it reached its maximum position or at least reached a sufficient height to continue the operation. The operations supervisor may have believed that since the mast had stopped, the control room operator had stopped the motion and was now waiting for the crane to hook to the electrode. The operations supervisor may have intended to notify the control room operator when the hooking operation was completed, as was the typical practice, rather than notifying the control room operator both at the beginning and the end of the hooking operation. He assumed that the crane operator was going to notify the control room operator that the electrode was hooked.

On the other hand, the failure of the electrode’s positioning system during this event was not a sole episode. This event had occurred in the past; thus, the operators created a nonstandard practice to deal with this condition. The engineers and supervisors, and the management knew about it, but they decided not to perform modifications to the PLC as they had concerns about its integrity due to its obsolescence. Thus, they decided to wait for the shutdown when the new PLC was planned to be installed. However, in the meantime, the engineers and supervisors did not review this practice to analyze how it could compromise safety.

The engineers and supervisors realized that the safety protections to avoid potential collision between moveable components of the furnace were out of service during the start-up. Moreover, some automatic sequences to perform the movement of the furnace components were also unavailable. They evaluated this situation and determined that they were not sufficient reasons to stop the startup process, so they decided to continue with it. However, the analysis was performed without adequately assessing the hazards that this decision could lead to.

Furthermore, the plant had a safety procedure indicating how to proceed in emergencies due to water leaks. However, it lacked enough detail to provide meaningful guidance to the operators about how to manage the emergency correctly during different scenarios. For example, it did not mention, in specifics, how to proceed in case of a severe water leak occurring in the furnace roof of the Fuchs EAF. The document only provided a general sequence to stop the furnace operations, and it requested to inform the maintenance team about the water leak to repair it.

Table 8: Analysis of loss at the control system level. Operations management

Operations Management
Safety Related Responsibilities • **SR-1:** Follow safety procedures and standards while performing their activities. • **SR-2:** Determine, correct, and report operational safety anomalies. • **SR-3:** Prioritize safety as the primary value of the company. No emergency, production process, or results justify putting people's occupational safety or health at risk. • **SR-4:** Review and approve operating procedures to control the hazards adequately. • **SR-5:** Oversee operations to ensure the (safety-related) policies and procedures are being followed. • **SR-6:** Ensure training to operation team on plant hazards and safe operating procedures. Audit to see if training has been effective. • **SR-7:** Promote adequate safety behaviors through an evident commitment to safety to prevent accidents and incidents. • **SR-8:** Ensure safe delivery of equipment conditions before shutdowns; Additionally, ensure a safe start-up after maintenance shutdowns. • **SR-9:** Review and approve the Safety Emergency Plan and ensure its compliance. • **SR-10:** Ensure the effective enforcement of the actions derived from investigations of accidents and incidents.

- **SR-11:** Propose an Investment Program on safety (FAI), aimed to reduce the hazards and risks within his/her area of responsibility.

Unsafe decisions and control actions

- **UCA-1:** Managers did not define as a standard requirement the performance of pre-startup safety review (PSSR) to check operational readiness, including systems, equipment integrity, and organizational factors. [SR-2, SR-3, SR-8].
- **UCA-2:** The management approved to continue the plant start-up despite the flaws in the automation to control the position of the furnace components (e.g., safety protections disabled). [SR-3, SR-8].
- **UCA-3:** The operations management did not establish a policy for the management of change to identify, manage, and control modifications to standard procedures or operational thresholds. For example, the nonstandard practice to deal with the electrode's positioning issue was not properly analyzed and documented. [SR-1, SR-2, SR-3, SR-5].
- **UCA-4:** The operations management did not proactively expand the hazard analysis from previous events to the Fuchs furnace. A similar incident previously occurred in the Danieli EAF. However, the analysis and lessons learned were not extrapolated to the Fuchs EAF (e.g., the need of an automatic system to control the cooling system remotely, the need of sensors to monitor the status of the cooling system). [SR-10].
- **UCA-5:** The operations management team did not prioritize the capital expenditures (CAPEX) according to formal risk evaluations. The investment plan priorities were defined according to the expertise, judgment, and requirements of the management. [SR-11].
- **UCA-6:** The management approved standard procedures inadequately detailed to perform critical tasks (e.g., what to do in case of a severe water leak). [SR-4, SR-5].
- **UCA-7:** The management did not request and validate the risk assessments before the execution of projects and modifications that were implemented during the shutdown. [SR-8].
- **UCA-8:** Underestimated the impacts of the modifications in the control room (change of location of the control room and change of HMIs). [UCA-12].

Process Model and Mental Flaws

- **PM-1:** The management may have believed the PSSR was not required since the operations team had enough experience in plant start-ups after maintenance shutdowns. [UCA-1].

- **PM-2:** They believed one of the goals of the start-up was to test the new features of the PLC and the new equipment, so problems were expected (e.g., inactive safety protections may have been not unusual). [UCA-2].
- **PM-3:** The operations management believed any relevant safety issues discovered during startup would be reported and reviewed by engineers and supervisors. [UCA-2].
- **PM-4:** They believed the management of change policy was necessary to control the constant changes and modifications in the plant. [UCA-3].
- **PM-5:** Management may have believed that the opportunity areas found in recent safety events were more related to isolated human errors or negligence rather than systemic factors. [UCA-4].
- **PM-6:** The management may have believed that the safety needs in the plant were obvious. Thus, no formal analysis was required to determine the priorities regarding safety for the CAPEX plan. [UCA-5].
- **PM-7:** The management believed the engineers and supervisor had developed detailed procedures. Therefore, they may have approved them without performing a meaningful check. [UCA-6].
- **PM-8:** The management believed the best option was to open the furnace roof since the water was getting into the furnace, even though this situation was not documented. [UCA-6].
- **PM-9:** The management may have believed that the risk assessments traditionally performed by the engineering team should be good enough to cover all the safety aspects. Therefore, they may not have exhaustively reviewed them to detect potential flaws. [UCA-7].
- **PM-10:** The management believed that the relocation of the control room would not be a problem for the operators. They did not consider the requirement to have a reference to validate the position of the electrode, as the operator used to have a tape on the glass of the control room. [UCA-8].

Context

- **C-1:** The PSSR was not a common practice in the organization. Normally, a mental check was performed previous or during the start-up process. This check relied on the expertise of the operators, supervisors, and engineers, including the managers. However, as the shutdown was behind schedule, the operators planned to participate in the start-up were not available. Therefore, the leading operators (the control room operator and the crane

operator) during that shift were relatively new in their positions (less than six months) and lacked enough expertise to face the start-up. [PM-1].

- **C-2:** For the management, having problems during the plant start-up was part of the process. They believed it was a good opportunity to test the new equipment to identify flaws in the design or during the installation. Therefore, problems were expected and considered in the start-up of the plant. [PM-2, PM-3].
- **C-3:** The management realized that a management of change policy was needed to control the continuous changes the organization faced. However, they had not achieved this purpose to set a standard mechanism to manage the change. [PM-4].
- **C-4:** The analysis of the safety events was focused more on physical and human factors, rather than systemic causes. This approach did not provide the envision to the company to understand the dynamics of events as a whole. Therefore, the causes were isolated and not extrapolated to other situations. [PM-5].
- **C-5:** The company did not have a formal process to prioritize investments according to risk assessments. Traditionally the prioritized projects were the ones related to high-risk safety events that had occurred in the company. [PM-6].
- **C-6:** All procedures, depending on the relevance, had to be approved at different levels of management. Managers were overwhelmed; Thus, like normal, they did not have the time to review in detail the procedures. [PM-7].
- **C-7:** When the water leak occurred, the plant manager realized that the amount of water getting into the furnace was significant. Thus, he decided that the furnace roof needed to be open in preparation for an imminent explosion. If an explosive reaction happened with the furnace closed, the damages to the furnace and to its surroundings, including people might have been worst. [PM-8].
- **C-8:** The engineering team typically performed risk assessments before the execution of projects. However, they were not rigorous and detailed in the assessment of the possible impacts the projects could have. [PM-9].

C-9: When the main control room was relocated, the visual reference used to validate the position of the electrode was lost. Since this verification was not documented in a standard procedure, it was not able to be tracked. The management may not have been aware of this need, so it was not requested for the project to have a mechanism to validate the position of the lower end of the electrode. [PM-10].

A similar event occurred previously at the same plant in the Danieli EAF. A detailed investigation of this incident was performed. The report concluded that to prevent explosive

reactions due to water leaks, an automatic system was needed to control the cooling valves. Also, the analysis recommended a monitoring system to detect water leaks promptly. However, although these actions also would have applied to the Fuchs EAF, they were only diagnosed and implemented in the Danieli EAF.

The organization executed some projects during the shutdown in order to improve the plant safety. For example, the installation of a new and more robust chemical package to reduce leak events. However, other relevant activities were not adequately prioritized to reduce the risk state of the plant. The management decided to continue operating knowing that in case of an emergency, the Fuchs furnace would not be able to close the cooling system rapidly. Moreover, this risk was underestimated, considering that a similar event happened in the other EAF some months previously.

Maintenance Team

The maintenance team is comprised of the technicians, contractors, leaders, supervisors, and the management. Management is an abstraction that includes the heads of mechanical and electrical maintenance, as well as the maintenance manager of the plant.

Table 9: Analysis of loss at the control system level. Maintenance technicians and contractors

Maintenance Technicians and Contractors
Safety Related Responsibilities • **SR-1:** Follow safety procedures and standards while performing their activities. • **SR-2:** Determine, correct, and report operational safety anomalies. • **SR-3:** Prioritize safety as the primary value of the company. No emergency, production process, or result justifies putting people's occupational safety or health at risk. • **SR-4:** Ensure safe delivery of equipment conditions before shutdowns; additionally, ensure a safe start-up after maintenance shutdowns. • **SR-5:** Maintain plant equipment in a safe condition. • **SR-6:** Always keep all emergency alarms and safety sensors operational.
Unsafe decisions and control actions • **UCA-1:** The maintenance technicians did not evaluate and informed to their superiors the risks that the modification in the piping over the roof could cause. [SR-4, SR-5].

- **UCA-2:** They did not verify that the evacuation emergency siren was operating before starting the plant start-up. [SR-6].

Process Model and Mental Flaws

- **PM-1:** The maintenance technicians believed the piping modification was only a minor change that would not have a negative impact on safety. The technicians thought the modification would indirectly improve safety as it could facilitate the repair in case of a water leak. [UCA-1].
- **PM-2:** They believed the start-up of the plant was an opportunity to test and validate the modifications made during the shutdown. [UCA-1].
- **PM-3:** The maintenance technician believed the emergency siren was going to be reconnected by the engineering team since they were conducting the control room revamping project. [UCA-2].

Context

- **C-1:** In the past, minor modifications to equipment were executed without proper documentation and hazard assessments. It was not adequately stated what kinds of modifications required documentation, and who was responsible for this activity. [PM-1].
- **C-2:** The shutdown had an extensive scope, and many types of equipment were intervened to perform preventive or corrective maintenance. The plant start-ups have traditionally been the opportunity for the maintenance team to verify the condition of the equipment after the maintenance. [PM-2].
- **C-3:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. [PM-2].
- **C-4:** The maintenance technicians were not aware of all details of the modifications the engineering team was conducting during the shutdown. In normal operations, the maintenance technicians were responsible to keep all alarms in operation, but as the control room revamping project was out of their scope, they did not ensure the emergency alarms were in place. [PM-3].

Table 10: Analysis of loss at the control system level. Maintenance leaders and supervisors

Maintenance Leaders and Supervisors
Safety Related Responsibilities
• **SR-1:** Follow safety procedures and standards while performing their activities.

- **SR-2:** Determine, correct, and report safety anomalies.
- **SR-3:** Prioritize safety as the primary value of the company. No emergency, production process, or result justifies putting people's occupational safety or health at risk.
- **SR-4:** Develop maintenance procedures to control hazards adequately.
- **SR-5:** Oversee maintenance activities to ensure the (safety-related) policies and procedures are being followed.
- **SR-6:** Provide training to the maintenance team on plant hazards and safety procedures. Audit to see if training has been effective.
- **SR-7:** Promote adequate safety behaviors through an evident commitment to safety to prevent accidents and incidents.
- **SR-8:** Ensure safe delivery of equipment conditions before shutdowns; additionally, ensure a safe start-up after maintenance shutdowns.
- **SR-9:** Maintain plant equipment in a safe condition.
- **SR-10:** Always keep all emergency alarms and safety sensors operational.
- **SR-11:** Ensure the management of the Contractors Safety within its area of responsibility.

Unsafe decisions and control actions

- **UCA-1:** The maintenance leaders and supervisors agreed to restart operations without performing a pre-startup safety review (PSSR) to check operational readiness, including systems and equipment integrity. [SR-2, SR-3, SR-8, SR-9].
- **UCA-2:** The maintenance leaders did not perform a meaningful risk assessment of the modification on the piping length over the furnace roof to identify potential risks. [SR-8, SR-9].

Process Model and Mental Flaws

- **PM-1:** They believed a formal PSSR was not required as the start-up process was typically the time to test and verify the condition of the equipment. [UCA-1].
- **PM-2:** They believed the piping modification was only a minor change that would not have a negative impact on safety. The maintenance team thought the modification would improve safety as it could facilitate its overhaul in case of a water leak. [UCA-2].

Context

- **C-1:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. A complete PSSR may have delayed more time the beginning of the plant start-up. [PM-1].
- **C-2:** A formal PSSR was not a requirement in the organization. However, the maintenance leaders and supervisors supported the operations teams through the mental check they performed before the start-up. This verification relied on the expertise primarily of the maintenance leaders and supervisors, as well the operations engineers and supervisors. [PM-1].
- **C-3:** The maintenance team did not have a robust policy for management of change. It was not clear what kind of modifications required documentation, and who was responsible for this activity. The maintenance leaders considered the modification of the roof piping as an improvement, but they did not perform a study to evaluate the potential shortcomings of this modification. [PM-2].

Table 11: Analysis of loss at the control system level. Maintenance management

Maintenance Management

Safety Related Responsibilities

- **SR-1:** Respect safety procedures and standards while performing their activities.
- **SR-2:** Determine, correct, and report safety anomalies.
- **SR-3:** Prioritize safety as the primary value of the company. No emergency, production process, or result justifies putting people's occupational safety or health at risk.
- **SR-4:** Review and approve maintenance procedures to control hazards adequately.
- **SR-5:** Oversee maintenance activities to ensure the (safety-related) policies and procedures are being followed.
- **SR-6:** Ensure training to the maintenance team on plant hazards and safety procedures. Audit to see if training has been effective.
- **SR-7:** Promote adequate safety behaviors through an evident commitment to safety to prevent accidents and incidents.
- **SR-8:** Ensure safe delivery of equipment conditions before shutdowns; additionally, ensure a safe start-up after maintenance shutdowns.
- **SR-9:** Ensure the effective enforcement of the actions derived from investigations of accidents and incidents.

- **SR-10:** Propose an Investment Program on safety (FAI), aimed to reduce the hazards and risks within his/her area of responsibility.
- **SR-11:** Manage resources to keep the plant equipment in a safe condition.
- **SR-12:** Ensure the management of the Contractors' Safety within its area of responsibility.

Unsafe decisions and control actions

- **UCA-1:** The maintenance management did not request the performance of a pre-startup safety review (PSSR) to check operational readiness, including systems and equipment integrity. [SR-2, SR-3, SR-8, SR-11].
- **UCA-2:** The maintenance management did not proactively extrapolate the analysis of similar events to the Fuchs furnace. [SR-10].
- **UCA-3:** The maintenance management may not have considered as a top priority the instrumentation of the cooling system, neither the need for an automatic system to control it remotely. [SR-11].
- **UCA-4:** The maintenance management did not request the performance of risk assessments for the modifications implemented during the shutdown. [SR-8, SR-12].

Process Model and Mental Flaws

- **PM-1:** The maintenance management believed the PSSR was not necessary as the start-up was the opportunity to test all equipment and the modifications implemented during the shutdown. [UCA-1].
- **PM-2:** The maintenance management may have believed that the causes identified in previous safety events were isolated, and not applicable to the Fuchs furnace. [UCA-2].
- **PM-3:** They may have believed that as there were no records of high-risk incidents related to water leaks, the needs of instrumentation or to automate the controlling valves were not as important as other priorities. [UCA-3].
- **PM-4:** They may have believed that the modifications implemented during the shutdown were irrelevant concerning safety (e.g., the piping modification in the furnace roof), so no safety assessment was needed. [UCA-4].

Context

- **C-1:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. [PM-1].
- **C-2**: The PSSR was not standard procedure in the organization. While the organization had discussed the convenience to implement it, it was not a requirement. [PM-1].

- **C-3:** The analysis of safety events was focused more on physical and human causes, rather than systemic factors. This situation inhibited the extrapolation of lessons learned from past events to have a proactive call to action. [PM-2].
- **C-4:** No high-risk incidents were recorded in the Fuchs related to water leaks. Thus, no red flags were rose regarding the cooling system at that time. [PM-3].

  C-5: The organization did not have a specification to define what was a minor modification, as well as if it required a risk assessment before its implementation. The maintenance management did not encourage the following of a policy for management of change. [PM-4].

Engineering Team

The engineering team is integrated by the engineering workers, the project managers, and engineering management. In this case, engineering management involves different positions, such as automation and construction managers.

Table 12: Analysis of loss at the control system level. Engineering worker

Engineering Worker
Safety Related Responsibilities • **SR-1:** Follow safety procedures and standards while performing their activities. • **SR-2:** Determine, correct, and report operational safety anomalies. • **SR-3:** Prioritize safety as the primary value of the company. No emergency, production process, or result justifies putting people's occupational safety or health at risk. • **SR-4:** Ensure safe delivery of equipment conditions before shutdowns; additionally, ensure a safe start-up after maintenance shutdowns. **Unsafe decisions and control actions** • **UCA-1:** The engineering workers agreed to begin the start-up process without ensuring the safety protections of the new PLC were enabled. [SR-2, SR-3, SR-8]. • **UCA-2:** The engineering workers did not perform extensive testing to detect potential flaws in the modifications implemented prior to their start-up. [SR-8]. • **UCA-3:** The engineering workers did not enable the safety protections in the new PLC to control the position of the furnace components. [SR-8].

- **UCA-4:** The engineering workers did not consider the requirement from operators to have a reference to validate the position of the lower end of the electrode. [SR-8].
- **UCA-5:** The engineering workers did not perform meaningful risk assessments to cover the possible failure scenarios for both the modifications and the newly implemented equipment. [SR-8].
- **UCA-6:** The engineering workers did not connect the evacuation emergency alarm in the new control room. [SR-4].

Process Model and Mental Flaws

- **PM-1:** The engineering workers realized that the safety protections were not activated when the start-up began, but they believed that it was safe to continue as the operations team had approved. [UCA-1].
- **PM-2:** They believed one of the goals of the start-up was to test the new features of the PLC, so finding inactive safety protections were not unusual. [UCA-1].
- **PM-3:** The engineering workers may have believed that performing trials before the start-up could disturb or affect the normal operations. [UCA-2].
- **PM-4:** The engineering workers unintentionally omitted the enable of the safety protections of the new PLC. They believed the protections were in place at the beginning of the start-up. [UCA-3].
- **PM-5:** The engineering workers may have believed that the requirement to have a visual reference was not relevant since the control room operator already had a position reference coming from the mast's encoder. [UCA-4].
- **PM-6:** They believed the risks assessments developed were good enough to prevent the failure scenarios they have considered as possible. [UCA-5].
- **PM-7:** They may have believed the evacuation emergency alarm was in place. [UCA-6].

Context

- **C-1:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. The operations teams agreed to continue the start-up as it was the opportunity to detect more potential flaws or problems. [PM-1].
- **C-2:** After extensive maintenance shutdowns, failures normally occurred, thus the organization accepted as normal to have problems during the start-up. The former PLC to control the furnace positions used to have restrictions to avoid collisions between movable components (e.g., between the electrode and the furnace roof). However, during the start-

up, the new PLC did not perform these restrictions, due to the engineering workers disabling them. [PM-2].

- **C-3:** The Fuchs furnace was one of the main production lines in the company. However, the engineering workers determine that it was not convenient to perform a test prior to the shutdown due to the critical condition of the PLC and the risks that it may imply. [PM-3].
- **C-4:** The engineering workers may not have had a robust verification process prior to the start-up of new equipment. They discovered the protections were not in place when the control room operator informed that he could move the furnace roof, even though the mast was not at its top position. [PM-4, PM-6].
- **C-5:** The engineering workers did not address the need to have a reference to validate the position of the electrode as they did not get the requirement from the operations team. [PM-5].
- **C-6:** At that time, robust engineering hazard assessments were not mandatorily performed before the project execution. The hazard assessments that were in used did not provide a reliable way to detect missing or incorrect requirements. [PM-2, PM-3, PM-5, PM-6].

The risk assessments performed by the engineering team prior to the implementation of projects was a relevant factor in the occurrence of the event. As stated earlier, the main control room was changed to make it more comfortable and safer by moving it further away from the furnace. When the engineering team changed its location, they did not consider that the operators had put a small tape on the front window as a reference of the electrode position. This missing reference was critical for the event that transpired as the operators did not have a visual aid to determine the position of the electrode concerning the roof pass line. The lack of detail in the engineering assessments could be due to the methods used to perform them. Traditional methods, such as 5 Why or Bowtie were unable to capture these needs.

Table 13: Analysis of loss at the control system level. Project manager

Project Manager
Safety Related Responsibilities • **SR-1:** Follow safety procedures and standards while performing their activities. • **SR-2:** Determine, correct, and report safety anomalies. • **SR-3:** Prioritize safety as the primary value of the company. No emergency, production process, or result justifies putting people's occupational safety or health at risk. • **SR-4:** Develop engineering procedures to control the hazards adequately.

- **SR-5:** Oversee project activities to ensure the (safety-related) policies and procedures are being followed.
- **SR-6:** Provide training to the engineering team on plant hazards and safety procedures. Audit to see if training has been effective.
- **SR-7:** Promote adequate safety behaviors through an evident commitment to safety to prevent accidents and incidents.
- **SR-8:** Ensure safe delivery of equipment conditions before shutdowns; Additionally, ensure a safe start-up after maintenance shutdowns.
- **SR-9:** Ensure the effective enforcement of the actions derived from investigations of accidents and incidents.
- **SR-10:** Ensure the management of the Contractors Safety is within its area of responsibility.
- **SR-11:** Create the project's technology package (Hazard Process Analysis, Layers of Protections, Operating Procedures, Maintenance Plans, Security reviews pre-start-up, training on-boarding).

Unsafe decisions and control actions

- **UCA-1:** The project manager did not define an effective mechanism to validate the performance of modifications, as well as the newly added equipment was according to design. [SR-4, SR-8, SR-11].
- **UCA-2:** The project manager approved the design and location of the new control room without ensuring all needs from the operations team were covered. [SR-8].
- **UCA-3:** The project manager may not have spent enough time to review that the risk assessments of the projects were meaningful. [SR-8].

Process Model and Mental Flaws

- **PM-1:** The project manager believed that the plant start-up was a good opportunity to detect the flaws in design or errors during the implementation of projects. [UCA-1].
- **PM-2:** The project manager believed that conduct trial tests prior to the shutdown could be dangerous as the condition of the former PLC was critical due to its obsolescence. [UCA-1].
- **PM-3:** The project manager believed they had collected all the requirements from the operations teams regarding the new control room. [UCA-2].
- **PM-4:** They project manager believed the risk assessments performed by the engineering workers were enough to prevent most of the possible failure scenarios. [UCA-3].

Context

- **C-1:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. As time was constrained, the time to test the modifications was shortened. Thus, the tests were conducted during the start-up. [PM-1].
- **C-2:** The condition of the former PLC to control the position of the furnace components was critical, so the engineering team, together with operations and maintenance, decided to wait for the shutdown to replace it. Therefore, there was no opportunity to perform tests before its implementation. [PM-2].
- **C-3:** The process to collect the requirements from operations or maintenance was not robust. Typically, the operative areas were overwhelmed with their daily activities, so they spent insufficient time to review the projects. However, the project manager tried to collect as much of the information as possible to develop the project. [PM-3].
- **C-4:** The project manager was overwhelmed with activities; Therefore, he may have had no time to check the risk assessments carefully. [PM-4].

Table 14: Analysis of loss at the control system level. Engineering management

Engineering Management
Safety Related Responsibilities • **SR-1:** Follow safety procedures and standards while performing their activities. • **SR-2:** Determine, correct, and report safety anomalies. • **SR-3:** Prioritize safety as the primary value of the company. No emergency, production process, or result justifies putting people's occupational safety or health at risk. • **SR-4:** Review and approve engineering procedures to control the hazards adequately. • **SR-5:** Oversee project activities to ensure the (safety-related) policies and procedures are being followed. • **SR-6:** Ensure training to the engineering team on plant hazards and safety procedures. Audit to see if training has been effective. • **SR-7:** Promote adequate safety behaviors through an evident commitment to safety to prevent accidents and incidents. • **SR-8:** Ensure safe delivery of equipment conditions before shutdowns; Additionally, ensure a safe start-up after maintenance shutdowns. • **SR-9:** Ensure the effective enforcement of the actions derived from investigations of accidents and incidents.

- **SR-10:** Propose an investment program on safety (FAI), aimed to reduce the hazards and risks within his/her area of responsibility.
- **SR-11:** Ensure the management of the Contractors Safety within its area of responsibility.
- **SR-12:** Create the project's technology package (Hazard Process Analysis, Layers of Protections, Operating Procedures, Maintenance Plans, Security reviews pre-start-up, Training/Onboarding).

Unsafe decisions and control actions

- **UCA-1:** The engineering management did not request to have a robust procedure to detect early flaws in projects. [SR-8, SR-12].
- **UCA-2:** The engineering management did not request to perform robust engineering hazard assessments to prevent potential accidents. [SR-8].
- **UCA-3:** The engineering management did not extrapolate the lessons learned from past safety events to prevent future accidents. [SR-9].
- **UCA-4:** The engineering management allocated CAPEX resources without performing a risk analysis to prioritize projects. [SR-10].

Process Model and Mental Flaws

- **PM-1:** The engineering management may have believed the reviews performed by the project managers and engineering workers were enough to prevent mishaps. [UCA-1].
- **PM-2:** The engineering management may have believed that the risk assessments conducted by the project manager were good enough. [UCA-2].
- **PM-3:** They may have believed that the causes of previous events were isolated human errors or negligence, rather than systemic factors. [UCA-3].
- **PM-4:** The engineering management may have believed that it was not necessary to perform a risk analysis to identify the investment priorities. [UCA-4].

Context

- **C-1:** The engineering team was overwhelmed with duties. A more robust procedure to validate the project designs would have implied more effort from the project managers and engineering workers. Thus, the management considered the processes at that time were good enough to prevent potential flaws and accidents. [PM-1].
- **C-2:** Similarly, more robust safety assessments would have demanded more time from an organization that was already overloaded with activities. The management may have

considered that the assessments performed had a good trade-off between the effort and quality and that they were sufficient to detect and prevent safety anomalies. [PM-2].

- **C-3:** A similar incident previously occurred in the Danieli furnace. The analysis, besides other aspects, recommended the instrumentation of the cooling system to monitor it actively. Additionally, the analysis recommended the installation of automated valves to shut-off the system in case of an emergency. Those recommendations also applied to the Fuchs furnace. However, other projects were prioritized over these needs. [PM-3].
- **C-4:** The organization did not have a formal process to prioritize the CAPEX for safety projects. Therefore, the allocation of resources was influenced by high-risk accidents that had occurred recently. Additionally, the benefits of safety investments were hard to be translated into economic terms. Thus, they may not have seen as attractive as other projects related to performance improvement. [PM-4].

Safety Team

The safety team is comprised of a slim structure integrated by the safety engineer and safety management. Safety management encompasses the head of safety of the plant and the safety manager.

Table 15: Analysis of loss at the control system level. Safety engineer

Safety Engineer
Safety Related Responsibilities • **SR-1:** Follow safety procedures and standards while performing their activities. • **SR-2:** Determine, correct, and report safety anomalies. • **SR-3:** Prioritize safety as the primary value of the company. No emergency, production process, or result justifies putting people's occupational safety or health at risk. • **SR-4:** Develop operation, maintenance, and engineering procedures to control hazards adequately. • **SR-5:** Oversee operation, maintenance, and project activities to ensure the (safety-related) policies and procedures are being followed. • **SR-6:** Provide training to the operations, maintenance, and engineering teams on plant hazards and safety procedures. Audit to see if training has been effective. • **SR-7:** Promote adequate safety behaviors through an evident commitment to safety to prevent accidents and incidents. • **SR-9:** Generate an effective Safety Emergency Plan and ensure its compliance.

- **SR-10:** Ensure the effective enforcement of the actions derived from investigations of accidents and incidents.
- **SR-11:** Participate actively as a reference for safety, providing technical support to the operation, maintenance, and engineering areas.

Unsafe decisions and control actions

- **UCA-1:** The safety engineer did not promote the pre-startup safety review (PSSR) to be a mandatory procedure to be performed prior to the start-ups. [SR-2, SR-3, SR-4, SR-5].
- **UCA-2:** The safety engineer did not assess the risks to perform nonstandard practices to deal with substandard conditions (for example, the workaround to deal with the electrode's positioning issue). [SR-1, SR-2, SR-3, SR-5].
- **UCA-3:** The safety engineer did not detail the emergency procedures to control water leaks. [SR-4].
- **UCA-4:** The safety engineer may not have followed up the lessons learned and action plans from previous similar events to apply them to other production lines. [SR-10].
- **UCA-5:** The safety engineer did not actively participate during the design and planning phase of the shutdown to detect the potential hazards related to the engineering or maintenance modifications. [SR-11].
- **UCA-6:** The safety engineer did not develop a meaningful risk assessment of the projects and modifications implemented during the shutdown. [SR-5].

Process Model and Mental Flaws

- **PM-1:** While the safety engineer believed the PSSR was a relevant procedure to manage the risks during a start-up, he believed it would require first the approval from the operations management. [UCA-1].
- **PM-2:** The safety engineer believed the workaround to deal with the electrode's positioning issue would not represent a safety issue. [UCA-2].
- **PM-3:** The safety engineer believed the emergency procedure to control the water leaks was adequate. It had been active for a long time and had been reviewed and approved by the management. [UCA-3].
- **PM-4:** The safety engineer may have believed that lessons learned from similar past events were considered in an improvement plan for the Fuchs furnace. [UCA-4].
- **PM-5:** The safety engineer may have believed that his participation during the design and planning phases of projects was not relevant, as typically the engineering team performed the safety assessments on their own. [UCA-5, UCA-6].

Context

- **C-1:** The operations team may not have been convinced about the need to have a specific procedure to check the readiness of the plant prior to its start-up. The safety engineer acknowledged this situation, and as the operations team had never performed this procedure, and there was no record about high-risk incidents related to this topic, the safety engineer did not insist on its relevance. [PM-1].
- **C-2:** The workaround to deal with the electrode's positioning issue became a normal practice for the operators. As it was performed recurrently without no relevant issues, over time, it created a false sense of security within the operations team and safety team. It was considered as a temporary solution which was planned to be solved during the shutdown. However, although the former PLC was replaced in the shutdown, the issue manifested during the start-up as the operations and engineering team did not properly address it. [PM-2].
- **C-3:** The emergency procedure that described what to do in case of a water leak had been reviewed and approved by the operations management. However, it did not include different failure scenarios, including what do in case of a severe water leak in the furnace roof. The fact that the management reviewed the procedure created false confidence that the procedure was complete. [PM-3].
- **C-4:** The lesson learned and recommendations from the incident in the Danieli furnace were shared to different levels and teams in the organization. The deficiencies on the cooling system of the Danieli furnace, regarding its monitoring and control, were prompt addresses by the organization. However, they were not addressed with the same sense of urgency on the Fuchs furnace, although the risk level was similar on both production lines. [PM-4].
- **C-5:** The safety engineer was coped with activities concerning occupational safety tasks rather than process safety. The safety structure was very lean, having only one engineer for the steelmaking process. He did not have sufficient time to participate in the engineering and safety assessments performed by the engineering team. [PM-5].

Table 16: Analysis of loss at the control system level. Safety management

Safety Management
Safety Related Responsibilities • **SR-1:** Determine, and report safety anomalies.

- **SR-2:** Prioritize safety as the primary value of the company. No emergency, production process, or result justifies putting people's occupational safety or health at risk.
- **SR-3:** Oversee operation, maintenance, and project activities to ensure the (safety-related) policies and procedures are being followed.
- **SR-4:** Ensure training to the operations, maintenance, and engineering teams on plant hazards and safety procedures. Audit to see if training has been effective.
- **SR-5:** Promote adequate safety behaviors through an evident commitment to safety to prevent accidents and incidents.
- **SR-6:** Review and approve the Safety Emergency Plans and ensure their compliance.
- **SR-7:** Ensure the effective enforcement of the actions derived from investigations of accidents and incidents.
- **SR-8:** Propose an investment program on safety (FAI), aimed to reduce the hazards and risks within his/her area of responsibility.
- **SR-9:** Participate actively as a reference for safety, providing technical support to the operation, maintenance, and engineering areas.
- **SR-10:** Define the safety policy and standards of the organization and ensure their communication and understanding of all members of the organization.
- **SR-11:** Share and communicate through all the organization safety events to raise safety awareness.

Unsafe decisions and control actions

- **UCA-1:** The safety management did not request the pre-startup safety review (PSSR) to be a mandatory procedure to be performed prior to the start-ups. [SR-2, SR-3].
- **UCA-2:** The safety management did not promote that the action plans from past events were expanded to other facilities with similar issues. [SR-7].
- **UCA-3:** The safety management did not define a robust policy of management of change to control the modifications adequately on facilities. [SR-10].
- **UCA-4:** The safety management may not have promoted the prioritization of CAPEX according to risk evaluations. [SR-8].
- **UCA-5:** The safety management did not define, as a requirement, the performance of robust engineering and safety assessments prior to the implementation of projects. [SR-10].
- **UCA-6:** The safety management may not have encouraged the active participation of the safety team during the design and planning phases of projects and shutdowns. [SR-9].

- **UCA-7:** The safety management did not establish the use of more comprehensive methods to analyze and prevent accidents. [SR-10].

Process Model and Mental Flaws

- **PM-1:** While the safety management believed the PSSR could be a helpful tool to manage the risks during a start-up, they believed it required the buy-in from the operations management to be effective. [UCA-1].
- **PM-2:** The safety management team believed the lesson learned and actions defined for previous events were known by the operations, maintenance, and engineering teams. [UCA-2].
- **PM-3:** The safety management believed the management of change should be an important milestone in the safety management of the organization. But they did not define how to achieve this goal. [UCA-3].
- **PM-**4: The safety management may have believed that the operations and engineering team controlled the CAPEX and that they did not have strong leverage to make recommendations. [UCA-4].
- **PM-5:** The safety management may have believed the assessments prepared by the safety engineers and the engineering team prior to the implementation of projects was good enough to prevent accidents. [UCA-5].
- **PM-6:** The safety management believed the safety engineers were deeply involved in the planning of projects and shutdowns. [UCA-6].
- **PM-7:** The safety management believed that the safety methods they were using (e.g. RCA) were good enough to understand the causality of the events. [UCA-7].

Context

- **C-1:** The idea to implement the PSSR after extensive shutdowns had been under the analysis of the organization for a long time. However, the organization may not have been fully convinced about the benefits that this practice could bring. The safety management did not push forward this plan. Instead, they focused on other aspects that they believed could have more impact on the safety performance of the company (e.g., identify and classify the activities performed by the operators according to their risk). [PM-1].
- **C-2:** The safety management may have considered that the analyses from past events were shared and available to the organizations. Therefore, the operations, maintenance, and engineering teams knew what the recommendations were, and which could apply to the Fuchs furnace as well. However, the safety management may not actively have

promoted the inclusion of the Fuchs furnace on the plan to solve the deficiencies of the cooling system of the other furnace. [PM-2].

- **C-3:** Management of change had been a topic that concerns the organization. However, safety management had not defined how to address this milestone to control the continuous changes in the process, systems, and equipment. For example, the modification of the piping length of the furnace roof was not followed by a risk assessment to address the potential impact of this modification. [PM-3].
- **C-4:** The safety management should have been a compass to guide the organization where to allocate the resources to improve the safety performance of the company. However, safety may not have played a significant role in the definition of the CAPEX of the organization. The definition of priorities was defined normally by the operations and engineering team. Thus, the prioritization could have had a bias towards other priorities such as productivity and economic returns. [PM-4].
- **C-5:** The safety management may have not had the time to review, in detail, the safety assessments developed by the safety engineers or the engineering team. Therefore, they would feel confident about the completeness of the assessments performed by them. [PM-5].
- **C-6:** The safety engineers normally participated in some meetings for shutdown planning. However, they did not get into details about the specifications of the modifications to validate if those modifications could increase the risk factors since they had other responsibilities. Similarly, the safety engineer participated briefly in the design phase. [PM-6].
- **C-7:** RCA has been the standard method to analyze accidents by the organization for several years. While the approach could be helpful to determine the causes of an accident, it has considerable limitations to understand the full dynamic of events in complex systems and large organizations. [PM-7].

Corporate Management Team

The corporate management team is an abstraction comprised of different corporate directors and top-level executives of the company.

Table 17: Analysis of loss at the control system level. Corporate management

Corporate Management
Safety Related Responsibilities • **SR-1:** Prioritize safety as the primary value of the company. No emergency, production process, or result justifies putting people's occupational safety or health at risk. • **SR-2:** Promote adequate safety behaviors through an evident commitment to safety to prevent accidents and incidents. • **SR-3:** Ensure the effective enforcement of the actions derived from investigations of accidents and incidents. • **SR-4:** Propose an Investment Program on safety (FAI), aimed to reduce the hazards and risks within his/her area of responsibility. • **SR-5:** Define the safety policy and standards of the organization and ensure their communication and understanding of all members of the organization. • **SR-6:** Share and communicate through all the organization safety events to raise safety awareness. • **SR-7:** Ensure that everyone who works in the company has adequate skills to perform their positions. • **SR-8:** Provide and allocate resources to ensure the compliance of safety policy and standards. **Unsafe decisions and control actions** • **UCA-1:** Did not require in-depth analysis of incidents and accidents that rigorously considered and emphasized systemic causes. [SR-10]. • **UCA-2:** The corporate management may not have allocated enough resources for implementing corrective actions broadly throughout other units. [SR-4, SR-8]. • **UCA-3:** Did not require robust engineering and safety assessments prior the CAPEX approval. [SR-4]. • **UCA-4**: May did not have adequately fostered a safety culture in the organization in which safety was prioritized over other goals. [SR-2]. **Process Model and Mental Flaws** • **PM-1:** Believed recent safety events were more related to isolated human errors or negligence than systemic factors. [UCA-1].

- **PM-2:** Believed the analysis performed by the engineering team to support the CAPEX request were adequate. [UCA-3].
- **PM-3:** Believed the organization was clear about safety was the priority and that their actions were aligned to this goal. [UCA-4].

Context

- **C-1:** The analyses of incidents and accidents were performed following a Root Cause Analysis method focusing more on physical (e.g., equipment failures) and human causes, rather than systemic causes. Similar incidents occurred previous to this event, but the lessons learned, and the action plans defined were not implemented in the Fuchs with a sense of urgency as in the Danieli furnace. Although both facilities had similar risk levels. [PM-1].
- **C-2:** The CAPEX requests had to include an engineering and safety assessment and had to pass through an extensive channel of approvals from different management levels. By the time the requests had reached the upper management, they have been reviewed by several people from different areas and hierarchical levels. Therefore, corporate management may have felt confident that the project was well supported and prioritized regarding safety. [PM-2].
- **C-3:** Management may have felt confident that the organization was engaged towards safety due to good results in the overall safety indicators of the company. However, they may not have had the right pulse of what was happening at the floor level, seeing if the people believed that safety was the main priority for the organization. [PM-3].

Once the UCAs have been described in detail, the following figures summarize the relationship between the UCAs and the control structure to demonstrate their occurrence at different organizational levels of the company. This envision allows to have a quick view of the unsafe actions connected to the event and to distinguish the most common.

Lower organizational level

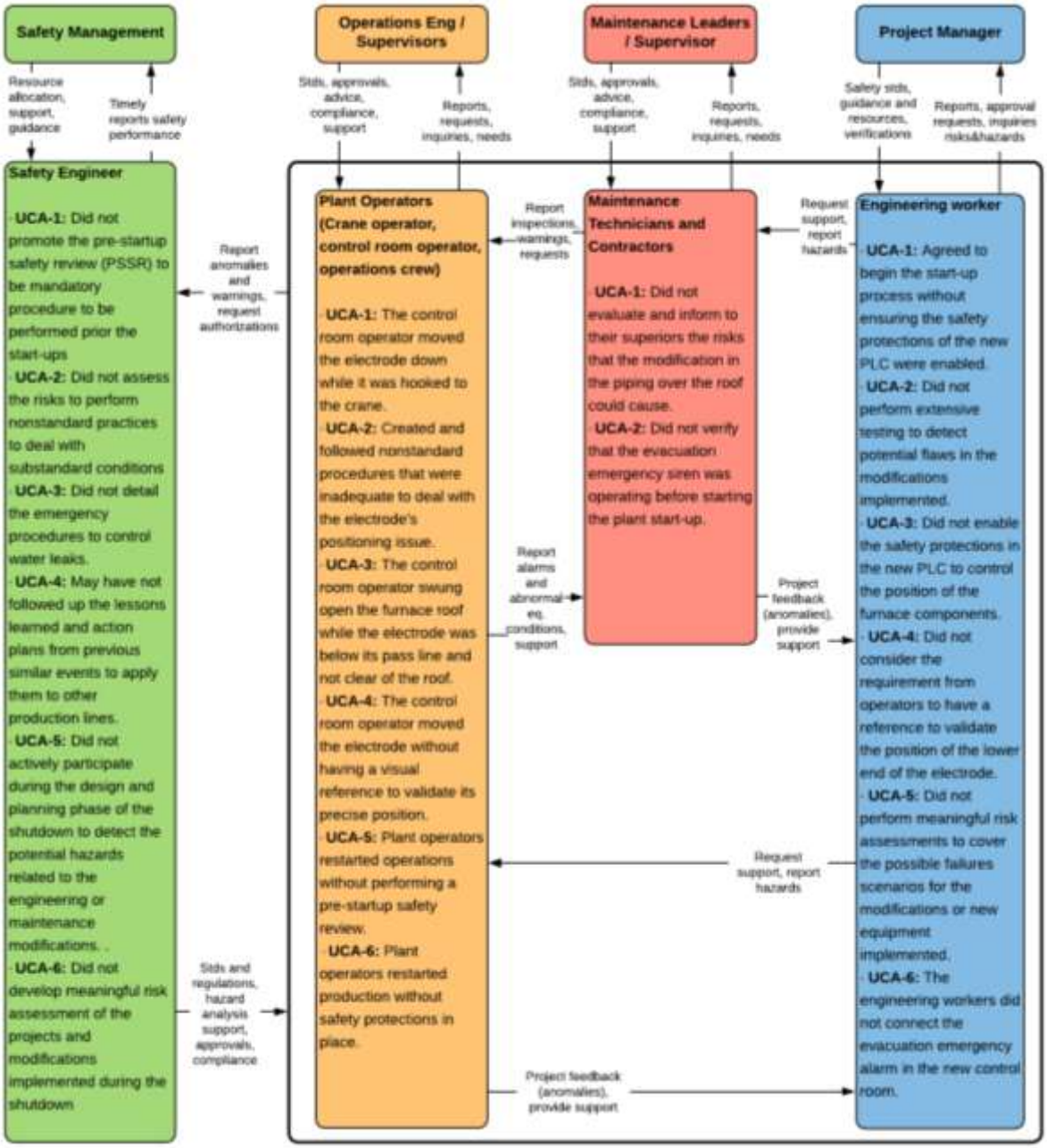


Figure 31: UCAs at the lower organizational level

Medium organizational level

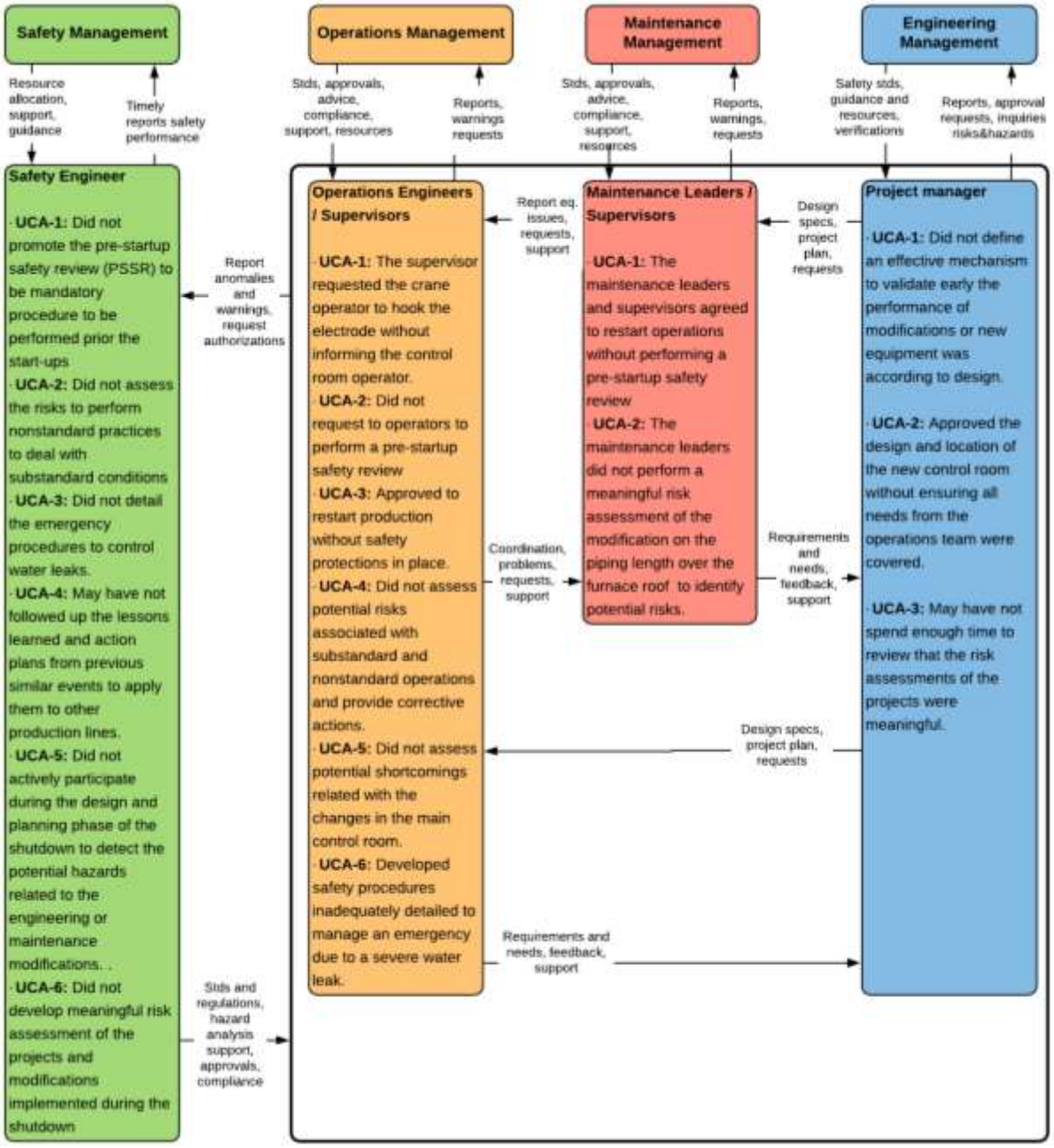


Figure 32: UCAs at the medium organizational level

Top organizational level

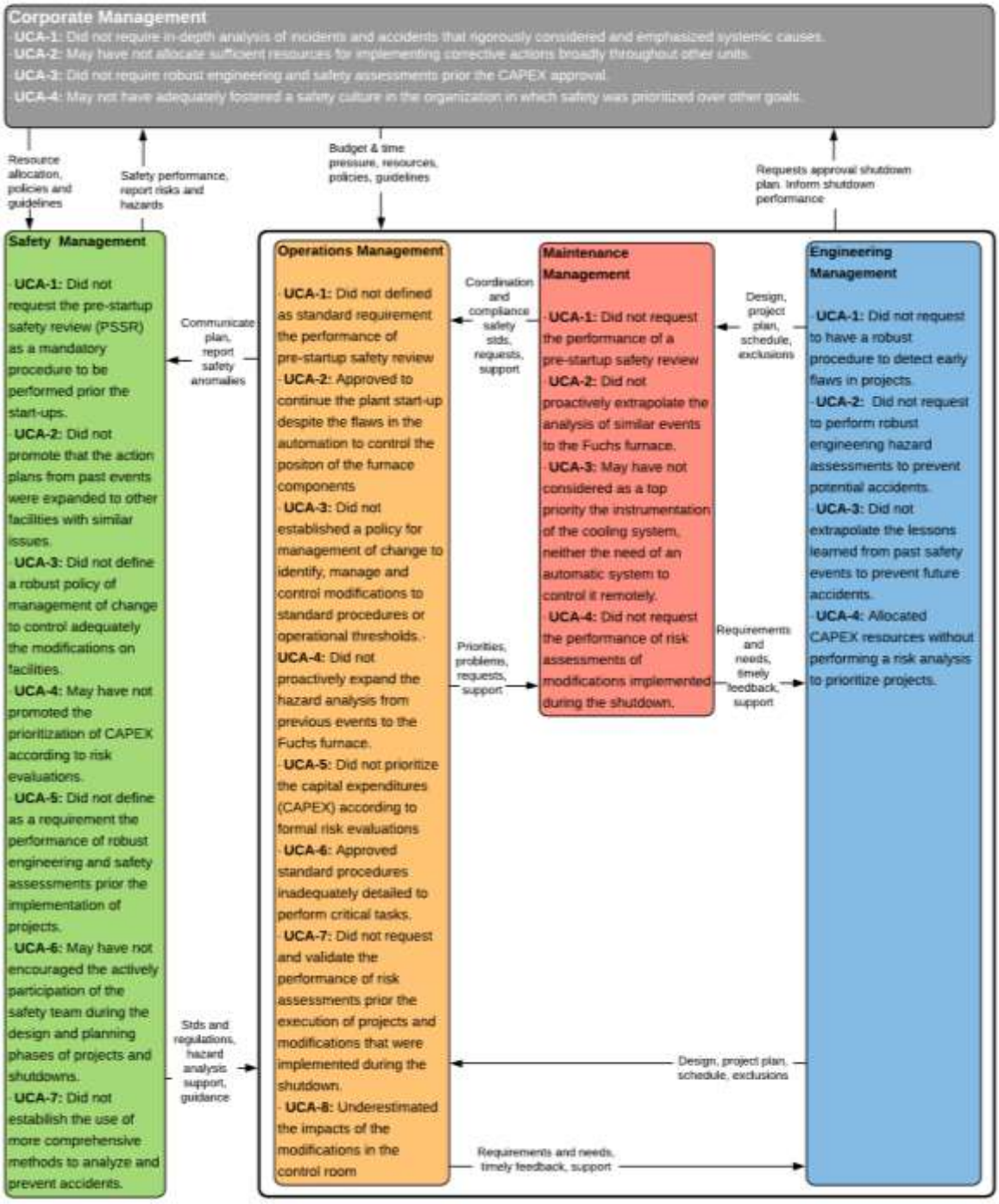


Figure 33: UCAs at the upper organizational level

The previous figures showed the unsafe control actions at different organizational levels in this analyzed system. While every UCA is specific to each controller, most of them can be

grouped in particular topics to identify the most common unsafe actions. In summary, the most common topics were:

- The performance of inadequately detailed risk assessment to prevent and mitigate possible failure scenarios in projects and modifications.
- The absence of a formal pre-start safety reviews process to ensure the readiness of the plants prior their start-up.
- The lack of a robust policy for management of change to validate and control the modifications performed within the organization.
- The lack of risk analysis to support the prioritization of the CAPEX allocation.
- The decision to restart operations knowing the safety flaws in systems (e.g. PLC safety protections disabled, issues with the electrode's positioning).

All the latter subjects are interconnected indicating the incident was not an isolated event but a result of system deficiencies within the company safety management.

One of the contextual factors that may had a catalyst effect was the pressure. Pressure is a common element within an organization. It usually has a negative connotation, but it could be an excellent incentive to improve and obtain faster results. The problem relies on when pressure distorts the operational and safety principles of organizations. Typically, under stressed circumstances is when it is evident the real culture of organizations.

In this case, as the pressure to restart operations grew due to the delays in the shutdown, the movement towards a riskier state manifested. Workers started to feel more stressed to closing maintenance activities and re-start operations; hence, the possibility of having an accident increased as people tended to be less focus on safety than timing. Adding to this, the inadequacies in the management of change related to the modifications in the control room and the piping over the furnace roof, and the flaws in the design of the control system, and the lack of procedures to validate the plant readiness, were some factors to create a hotbed to cause an accident.

One of the remarkable positive aspects of this incident was that even though its potential, no person was harm due to the reactions. This positive facet was related to the decision of the company to install safety gates to surround the furnaces areas; so, at the moment of the incident, very few people were close to the furnace. This critical decision was a fundamental factor to avoid personal damages.

4.4.7 Coordination and communication contributors

Communication is a critical factor in safety management. An organization could be proud of its safety values and core principles; however, it is essential that these values are communicated downward through all organizational levels.

Good communication allows an open flow of exchanging information, especially upwards through the top-level management. This process does not spontaneously appear; it is based on a trustworthy environment built upon the coherence, credibility, and genuine commitment from the organization. It frequently requires a significant amount of time to be created.

In this case, pressure could have been a factor that prevented the making of right decisions towards safety. A strong safety culture is resilient to short-time temptations such as prioritizing the production over safety. The organization requires dedication towards the commitment of prioritized safety. They must make this clear across its operations, no matter what the circumstances are.

On the other hand, at the operational level, there were some opportunities to improve. It was mentioned early in this document that since the plant was in its restarting process, the radio frequencies used to communicate were continuously busy, which could have prompted to cause an accident due to misunderstandings or missing information. This fact was particularly important, since some activities such as changing the electrode, required precise coordination between operators due to deficiencies in the positioning control system.

The following figure shows in a simplified way the communication links and interactions at the time of the incident.

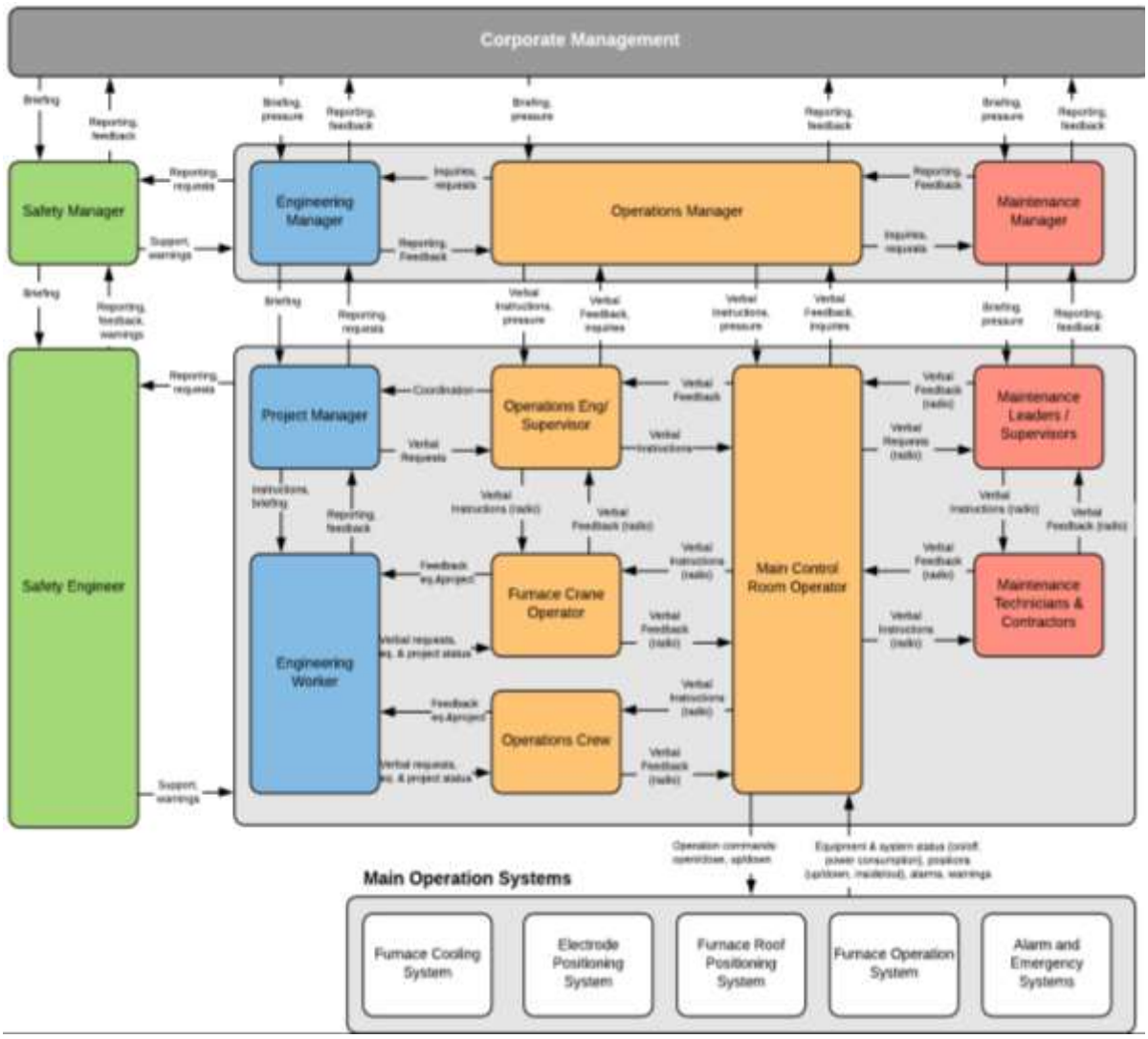


Figure 34: Communication links in the system

It is evident from the last figure, how relevant was the main control room operator during the re-start up process. He interacted to most of the human controllers of the system, regardless their organizational function and level. These communication links contrast to the normal communication dynamics exemplified in Figure 30. For comparison purposes, the following figure represents an extract of the Figure 30 focusing on the interactions of the main control room operator prior the start-up process.

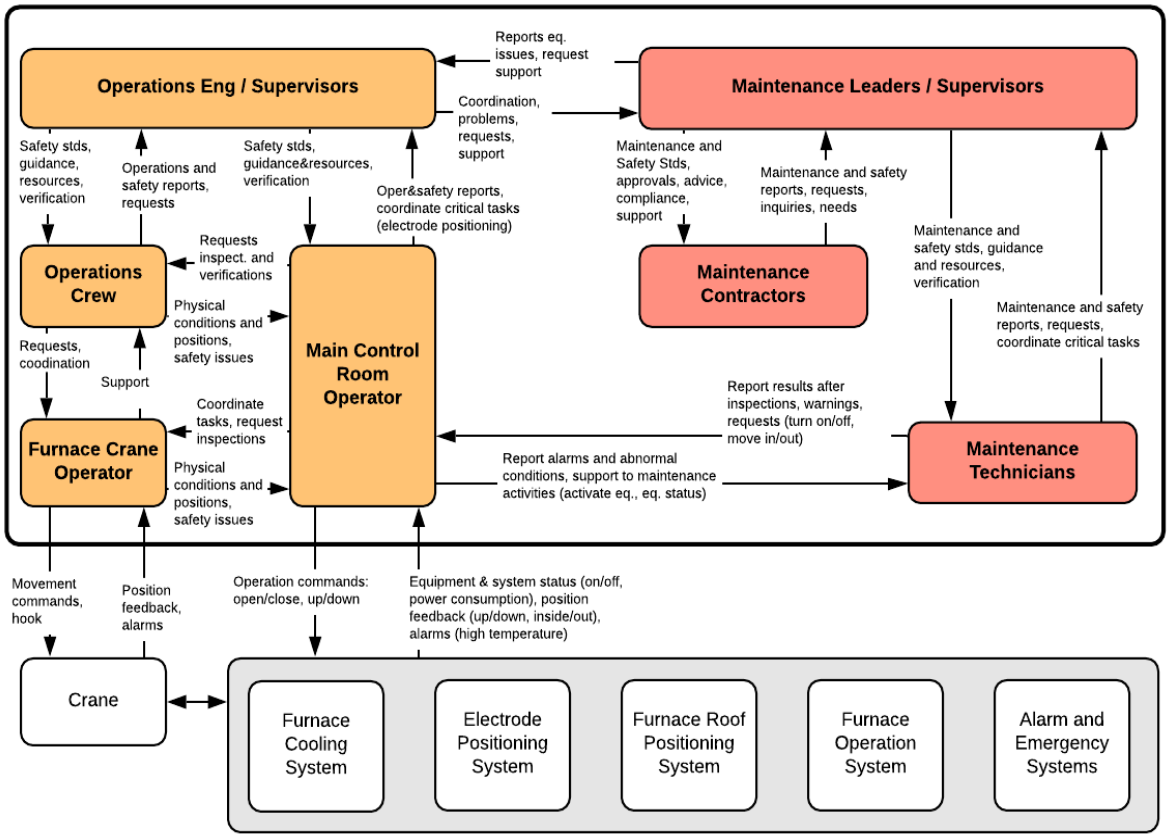


Figure 35: Extract of control structure of operations and maintenance team from Figure 30

In Figure 35 is noticeable how before the plant start-up the interactions of the control room operator remained basically at his organizational level. However, the main control room operator acted practically as the pivot of all operations. Typically, during the plant start-ups, the main control room turned into a war room since most of the operations are controlled and monitored through the HMIs. Thus, the control room operator was a fundamental element in this process. He had to coordinate activities, give instructions to the operations crew, and provide feedback about the current status of process and tasks to the maintenance and engineering team. This multitask facet of the control room operator, in combination with a stressful environment, were an amalgam to increase the operations risk.

Additionally, this figure shows the interactions between the main control room operator and the different operating systems. This subject was particularly important since all of the former HMI were changed during the shutdown, so the plant restarted operations with new interfaces. This made it harder for the control room operator to react accordingly in case of an emergency.

4.4.8 Dynamics and changes in the system over time

Safety events typically have precursors that are red flags alerting a degradation in safety. These red flags need to be promptly addressed as organizations do not know for sure when and where an accident might occur. In a good scenario, the organization acknowledges that something is happening and needs to be corrected; the most crucial problem takes place when organizations do not recognize these precursors or do not analyze them in-depth.

In addition to the communication opportunities revealed in the last section, other dynamics contributed to this incident, as explained in the following lines.

Equipment

The Fuchs electric arc furnace was the first furnace installed in the plant in the 1990s. Along the years, the company had made several modifications to improve its reliability and productivity through diverse investments, particularly in automation.

However, still, several activities needed to be performed manually or without sophisticated technologies. To address this situation, the company conducted a study to identify and prioritize the addition of modifications and new equipment needed to reduce the technological gap of facilities mainly to reduce the workforce exposure level.

The study identified several activities that could be improved through new technologies available in the market. Several modifications were implemented according to the recommendations from this study in the last years with notable results. Nevertheless, the requirement to implement an automatic control to close the cooling system rapidly in case of an abrupt water leak was not identified.

Similarly, many operational sequences needed to be performed manually or semi-automatically by the control room operator. Thus, the control room operator needed to be highly concentrated in the operation, and tightly coordinated with the rest of the crew to perform the required activities.

Risk management

In 2016, a similar incident occurred in the company. The incident was caused by a water leak in the Danieli EAF occurred without personnel injured. This event was a significant red flag for the company, and a reinforcement that some risks had not been adequately addressed.

After this event, some quick actions were implemented, such as the installation of cameras to detect water leaks in both EAFs. Additionally, some projects with inherent safety benefits were

executed during the maintenance shutdown. For example, the relocation of the control room further away of the furnace and reinforce it with ballistic windows to shield it in case of an explosive reaction (which in this case resulted in being paramount to avoid an accident). Also, the installation of a new chemical package to reduce the risk of water leaks into the furnace.

Nevertheless, some other projects required more time to be analyzed, designed, and implemented; two of these projects were the installation of automatic valves to control the cooling system remotely in the Fuchs furnace, and a set of sensors to monitor the condition of the cooling system. These projects were in the backlog of the engineering team.

4.4.9 Recommendations

After having developed the CAST analysis, a set of recommendations is provided to tackle the causes that led to this event, as well prevent similar events in the future. This list does not attempt to evaluate which actions are more critical than others. As previously noted, the CAST analysis provides a holistic picture of the factors and their relationship that may lead to the cause of this event.

The list is divided into seven parts: physical equipment and system design; procedures and routines; general recommendations; specific recommendations for operations team, maintenance team, engineering team, safety team, and corporate management. The tables also show which system constraint (SC) and unsafe control action (UCA) is addressed by the recommendation. This traceability is important to enable the results to be reviewed more effectively and to demonstrate that the suggested recommendations address the identified UCAs and Safety Constraints in the analysis.

Table 18: Recommendations for physical equipment and system design

Physical Equipment and System Design	**SC / UCA**
• Improve the robustness of the electrode positioning system by adding an alternate mechanism to detect if it has reached its maximum position.	SC-5 UCA-4 (Op Operator)
• Provide to the control room operator an adequate system to monitor the position of the lower end of the electrode. A visual inspection could serve as a reference, but alone it is not an effective control measure.	SC-5 UCA-4 (Eng Tech)
• Verify the control logic for the roof movement. It must have protection to avoid collision between the roof and the electrode.	SC-5 UCA-3 (Op Operator) UCA-3 (Eng Tech)
• Identify the sequences currently performed manually by the control room operator and evaluate potential automation of them. Perform a hazard assessment to determine the adequate constraints and restrictions to avoid collisions and possible errors.	SC-5 UCA-1 (Op Operator) UCA-3 (Eng Tech)
• Improve the protection of the piping in the roof cooling system. The piping should have robust construction and it should be covered to prevent damages if an object fell and crashed into it.	SC-1, SC-5 UCA-5 (Op Mng)

• Install a system to control the valves of the cooling system quickly and remotely (e.g. shut-off valves).	SC-2, SC-3, SC-4 UCA-5 (Op Mng)
• Provide online monitoring of the operational condition of the cooling system by adding sensors (e.g. flow, pressure, temperature) to detect leaks in the system. Be aware to no flood the operators with alarms. An adequate alarm management is critical to effectively prevent safety events.	SC-2, SC-3, SC-4
• Ensure the HMIs provide all the commands the operator needs to perform his/her tasks. Perform a hazard analysis using an appropriate method capable of addressing human factors concerns including potential sources of human confusion.	UCA-3 (Op Mng)

Table 19: Recommendations for procedures and routines

Procedures and routines	**SC - UCA**

• Develop a systematic process for evaluating operation readiness and integrity of equipment and system before and during restart operations from a shutdown to ensure all the critical equipment and controls operate adequately. The scope of the evaluation should include:
  • Critical equipment
  • Control systems (focus on critical sequences, safety protections and tasks regarding safety)
  • Human factors (for example, competency of workers, overtime)
	SC-5, SC-7
	UCA5,6 (Op. Operator)
	UCA-2,3 (Op Eng&Sup)
	UCA-1,2 (Op Mng)
	UCA-1,2 (Mnt Tech)
	UCA-1 (Mnt Ldr&Sup)
	UCA-1 (Mnt Mng)
	UCA-1 (Eng Tech)
	UCA-1 (Safety Eng)
	UCA-1 (Safety Mng)

• Check the emergency action plan, including emergency procedures and evacuation routes. Ensure all the personnel are familiar with it and receive corresponding employee training.	SC-6, SC-7 UCA-6 (Op Eng&Sup) UCA-6 (Op Mng) UCA-2 (Mnt Tech) UCA-6 (Eng Tech)

Table 20: General recommendations

General recommendations	**SC - UCA**
• Ensure adequate management of change addressing documentation, communication of risks, control measures, and	UCA-4,5 (Op Eng&Sup) UCA-3,7,8 (Op Mng)

needs of training/skills. Changes should be supported by hazard assessments to ensure the modifications are safe.	UCA-1 (Mnt Tech) UCA-2,4 (Mnt Ldr&Sup) UCA-5 (Eng Tech) UCA-3 (Eng PM) UCA-3,5 (Safety Mng)
• Ensure recommendations from previous safety events are implemented, and the lessons learned from internal and external events are shared within the organization.	UCA-4 (Op Mng) UCA-2 (Mnt Mng) UCA-3 (Eng Mng) UCA-4 (Safety Eng) UCA-2 (Safety Mng)
• Assign regular audits and periodic monitoring (maybe once a month) of control room operations to detect whether unreported control system errors are happening and identify unreported workarounds.	UCA-2 (Op Operator) UCA-4 (Op Eng&Sup) UCA-2 (Safety Eng)
• Foster a culture free of blame. The organization needs to build an open and constructive culture to radically transform its safety performance. Encourage reporting by guaranteeing that operators may not be punished for reporting flaws and workarounds (punishing will ensure that this information is never reported, and the benefits from getting the true information are more important than any benefit from punishment). If workarounds and control system errors are discovered that were not reported, determine the reason they were not reported and fix it (e.g. the reason may be that the reporting tool is too difficult to use or that operators feel like the reports go into a black hole and have no effect or follow-up, so why bother.)	UCA-2 (Op Operator) UCA-2 (Safety Eng)
• Establish open forums to discuss safety topics and concerns about safety at work. These forums could be a good opportunity to bring together the employees to build community. Define a regular frequency to have them (e.g. once a month).	N/A
• Create a small working group, including a representative from operations and from automation, to periodically review the reports and generate corrective actions to address the reports.	N/A
• Periodically calculate a statistic from the reporting tool to determine how many nonstandard workarounds have had to be	UCA-2 (Op Operator) UCA-2 (Safety Eng)

created and used by operators to get their job done, as well as a statistic about the number of and the potential severity of control system malfunctions. Ensure that supervisors, managers, and upper management is notified every month about this so that they understand the deficiencies in the system, whether they are being fixed, and whether new deficiencies are being introduced.	
• Define a review frequency for documentation to detect inconsistencies or updating needs. While there is not a criteria or standard frequency to revise documentation, a good practice is to have a regular time frame to perform this process (e.g. every year or two years). The documentation review should be an ongoing process in the sense that if a modification is required because something has changed in the operation, the procedures must be promptly updated.	UCA-2 (Op Operator) UCA-6 (Op Eng&Sup) UCA-6 (Op Mng) UCA-3 (Safety Eng)
• Change the methods used for incident and accident analysis. Similar incidents had already happened before, but the existing RCA method did not result in adequate learning from previous similar events and was not effective in preventing similar accidents like this one. Incidents and accidents must be investigated and analyzed with methods that can systematically uncover not only physical and human causes but organization factors, management beliefs, broken feedback in the system, and other systematic factors. The organization needs more effective methods for incident and accident analysis, such as CAST or equivalent.	UCA-7 (Safety Mng) UCA-1 (Corp Mng)
• Prioritize CAPEX according to risk assessments. The assessments would be a guide to effectively allocate them to reduce the overall safety state of the organization.	UCA-5 (Op Mng) UCA-3 (Mnt Mng) UCA-4 (Eng Mng) UCA-4 (Safety Mng) UCA-2 (Corp Mng)
• Reinforce the operator's skills through simulation training of emergency situations. This method could facilitate the learning process and increase the effectiveness of training to ensure an adequate response in case of critical circumstances (e.g. severe water leak).	UCA-1 (Op Operator) UCA-1 (Op Eng&Sup)

Table 21: Specific recommendations to operations team

Operations Team	SC - UCA
• Request, whenever as possible, a trial version of a new system to run in parallel to current systems before their full deployment to detect flaws that may cause an incident or accident.	UCA-7 (Op Mng)
• Demonstrate the commitment of management towards safety by having a frequent and visible presence at plant floor (e.g. at least one per week). Speak to workers, have positive approaches and gentle corrective inquires.	N/A
• Establish a suggestion box to foster the generation of innovative ideas to improve the safety performance of the facility. This suggestion box could be anonymous to collect concerns about safety that otherwise would not get to the management.	N/A

Table 22: Specific recommendations to maintenance team

Maintenance Team	SC - UCA
• Create a list of critical equipment for safety. Ensure testing, inspection, and maintenance program is effective.	SC-1, SC-2

Table 23: Specific recommendations to engineering team

Engineering Team	SC - UCA
• Adopt more effective methods for hazard analysis of the technological package before the execution of investments. The current method was ineffective in detecting or preventing the control system errors. (This recommendation and a path forward is examined in much more detail in Chapter 6)	UCA-4 (Eng Tech) UCA-2 (Eng Mng)
• Provide, whenever possible, a system trial version running in parallel to current systems before their full deployment to detect flaws that may cause an incident or accident.	UCA-1 (Eng PM) UCA-1 (Eng Mng)
• Establish a robust procedure to ensure a meaningful collection of needs and requirements from the project's stakeholders. Define regular meetings to communicate the project progress and verify if requirements need updating.	UCA-2 (Eng PM)

Table 24: Specific recommendations to safety team

Safety Team	**SC - UCA**
• Participate more actively in safety assessments of projects and maintenance shutdown plans. The participation of safety team in these activities is important to ensure the decisions taken are robust regarding safety.	UCA-5,6 (Safety Eng) UCA-6 (Safety Mng)
• Safety management should distribute lessons learned from accidents and incidents and sharing experiences on safety throughout the organization.	UCA-4 (Safety Eng)

Table 25: Specific recommendations to corporate team

Corporate Management	**SC - UCA**
• Understand concepts of process hazards, broken feedback loops in an organization, and systemic factors that contribute to accidents. Knowing the fundamentals of these concepts would increase the awareness of the importance of process safety.	N/A
• Establish regularly scheduled town hall meetings (e.g. quarterly meetings) to communicate the safety performance results, and more importantly, to communicate and align the vision of the organization towards safety. These meetings should be a good opportunity to interact with the employees and to hear directly from them their concerns about safety.	UCA-4 (Corp Mng)

This significant list aims to provide a guide to the management to address the specific and systems reasons that may lead to this event in the company.

The role of leadership is fundamental to achieve a transformation of the safety culture in the company. Studies have shown that top management's support for and participation in safety efforts are the most effective way to control and reduce accidents [3].

The organization needs to visualize safety not only as a priority, but as a way to conduct business. Safety is a living value that needs to be shared and acknowledged by all members of the company, including contractors.

Although the safety performance of the company reflects substantial improvements over the last years, events like this merit a stop on the way to perform a critical diagnosis about what

is happening, and what are the underlying reasons causing the high-risk events that could lead to critical losses.

Ironically, continued achievements could lead organizations towards a state of complacency, which may hinder its capacity to further improvements. This phenomenon is explained through the physiological concept of the avoidance paradox, which explains in simple terms that the safer we have been, the less safe we become, until injuries or process disasters occur sporadically and re-motivate avoidance [21]. Unfortunately, this phenomenon is more common than expected in the industry. Organizations need to be continuously intrigued about how to improve their safety management and not to fall into temptations to be eclipsed by good metrics.

4.4.10 Additional facts uncovered while applying CAST

While performing CAST, several facts that were missing in the official report were uncovered. They provided meaningful insights to have a better understanding of the safety dynamics of the incident. Some of the most remarkable information gathered was:

- The main control room was revamped and relocated during the shutdown. The new control room was placed further away from the furnace for safety purposes. Also, the HMIs of the control room were replaced during the shutdown by the new company standardized interfaces.
- It was not the first time that the electrode did not reach its top position. The practice to manually move the electrode was a common practice.
- During the restart of the plant, some of the automatic sequences and protections were not available or did not work correctly. For example, the protection to restrict the movement of the furnace roof in case the electrode was not in its top position was disable.
- The piping of the roof cooling system was modified by the maintenance team during the shutdown to facilitate future interventions. The length of piping connections was enlarged to avoid being cover by dust. However, this modification made the piping to be more exposed to damages from fallen objects.
- The crane operator and the main control room operator had both less than six months of experience on their positions, which was not unusual and did not violate any company policy at the time.
- The plant was under a stressful environment as the maintenance shutdown was delayed versus the original schedule.

- As the furnace was restarting operations, no workers were close to the furnace. The company previously had restricted the access to the adjacent areas of the furnace as a safety measure in case of an emergency.
- The water leak was controlled by turning down the centralized pumps of the cooling system. The valves of the furnace cooling system were not designed to be closed quickly or remotely, requiring significant time to close and delaying the response to the critical water leak. The centralized pumps were not exclusive for the cooling system of the furnace; they supplied water to other facilities in the plant.
- The evacuation protocol was executed when the incident occurred; however, the emergency siren was inoperable because it had been disconnected during the activities to relocate the main control room.

This additional information was important to understand the nature of this event and to develop more effective recommendations. One of the biggest concerns in any accident analysis is that critical factors might have been overlooked, allowing weaknesses in the system to continue to contribute to future accidents. In this case study, CAST was demonstrated to provide a systemic method that raises new questions, identifies previously overlooked causes, and provides a holistic view of the accident including the underlying systemic causes that shape human behavior, not simply blaming or identifying failed components.

The following chapter provides a comparison between the outcomes obtained using CAST and the results from the Root Cause Analysis performed by the company where this incident occurred.

Chapter 5: Comparison between CAST and Root Cause Analysis

This chapter aims to compare and contrast the analysis derived from using the Root Cause Analysis model performed by the organization, and the outcomes from the CAST model performed in this thesis.

5.1 Classification of causes

The Root Cause Analysis performed by the company considers three clusters of causes to cover the dynamics of the incident:

- Physical Causes
- Human Causes
- Systemic Causes

The first cluster describes the physical elements that failed, were inoperable, or were missing during the event; for example, the failure of a position sensor or the lack of redundancy in a specific control.

The second cluster describes the human causes. This cluster includes the causes the organization considers directly related to people's responsibility; for example, not following procedures adequately or the lack of coordination between operators. Finally, the third cluster encompasses systemic causes. This cluster seeks to capture the causes the company considered to be structural deficiencies that lead to the event. For example, deficiencies in training programs or inadequate controls in system design.

The standard Root Cause Analysis used by the company then identifies a list of actions to correct the causes detected under this model.

In contrast, the CAST analysis seeks to identify a broader set of causes across the physical level, the human operator level, and the organizational level. CAST identifies specific actions and decisions by each of these controllers that contributed to an accident, identifies why those actions and decisions seemed reasonable at the time through process model or mental model beliefs, and identifies contextual factors that influenced the behavior and that represent weaknesses in the broader socio-technical system. CAST seeks to provide a more holistic

perspective to understand the full dynamics of the incident across all levels of control, including deeper systemic factors that can be easily overlooked with a more ad-hoc analysis.

For comparison purposes, the following table shows a vis-à-vis perspective of the identified causes from both models. The following table summarizes this comparison:

Table 26: Comparison of factors detected between the RCA performed by the company and CAST, taking RCA as baseline

Root Cause Analysis (RCA)	Relationship RCA - CAST
Physical Causes (PC-#): **PC-1:** The main control room changed was moved during the shutdown to a safer position. However, the visual reference the operators used to identify the electrode position was lost after this change.	UCA-5 (Operations Eng&Sup) UCA-8 (Operations Mgmt) UCA-4 (Engineering Worker) UCA-2 (Engineering PM)
PC-2: The position of the roof while opened remained close to the furnace, causing the water leak to get quickly into the furnace.	FIC-4 (Physical System Level)
PC-3: The valves of the cooling system were not possible to operate from the control room. The valves were manual; hence, the reaction time to close them was significant.	FIC-2 (Physical System Level) UCA-4 (Operations Mgmt) UCA-3 (Maintenance Mgmt) UCA-3 (Engineering Mgmt) UCA-4 (Safety Eng)
Systemic Causes (SysC-#): **SysC-1:** During the tapping sequence, the electrode did not reach its top position at 649cm; it raised only to 618cm.	FIC-6 (Physical System Level)
SysC-2: The control room operator lowered 30 cm, the electrode mast since he noticed it did not reach its top position. He lowered the mast to enable the control.	UCA-1 (Operations Operator) UCA-4 (Operations Eng&Sup)
SysC-3: Weak control system, as the control room operator could activate the roof-swing sequence while the electrode was not in its top position.	FIC-5 (Physical System Level) UCA-3 (Operations Operator))

SysC-4: Uncommon operation since the plant was during its start-up process after an extensive shutdown with several technological changes.	This is not a cause. However, this contextual factors is addressed in CAST
Human Causes (HC-#): **HC-1:** Inadequate communication between the crane operator, operations supervisor, and the control room operator.	UCA-1 (Operations Operator) UCA-1 (Operations Eng&Sup)

The previous table was helpful as an overall comparison. All factors identified in the RCA were addressed by CAST. However, as this table took the RCA analysis as baseline, it only compares into one direction. To contrast all the factors considered by CAST in comparison to the ones considered by RCA, a new table is needed to represent this:

Table 27: Comparison between CAST and RCA performed by the company, taking CAST as baseline

CAST factors		RCA Causes
Physical System Level		
Failures and inadequate controls in the physical equipment	· **FIC-1:** The operators were unable to monitor the status of the cooling system. [PCE-1].	-
	· **FIC-2:** The operators were unable to shut down the cooling system in case of an emergency. [PC-2].	PC-3
	· **FIC-3:** The piping over the furnace roof was damaged by a fallen object. The damage caused the water leak. [PCE-6].	-
	· **FIC-4:** The position of the roof while opened remained close to the furnace, causing the water leak to get quickly into the furnace. [PCE-5].	PC-2
	· **FIC-5:** The PLC did not avoid the collision between furnace components (e.g. roof and electrode). [PCE-7].	SysC-3
	· **FIC-6:** The mast failed to reach its top position when the operator extracted the electrode from the furnace's inside. [PCE-8].	SysC-1
	· **FIC-7:** The operator did not receive an alert on the HMI about the potential collision between the roof and the electrode when he moved the roof to its open position. [PCE-9].	-
	· **FIC-8:** The operator did not have adequate feedback to determine the precise position of the lower part of the electrode. [PCE-7].	-
	· **FIC-9:** The audible evacuation signal did not sound when the operator tried to activate it. [PCE-10].	-
Plant Operators (Crane operator, Main control room operator, Operations crew)		
Unsafe decisio	· **UCA-1:** The control room operator moved the electrode down while it was hooked to the crane. [SR-1].	SysC-2

	· **UCA-2:** Operators created and followed nonstandard procedures that were inadequate to deal with the electrode's positioning issue. [SR-1, SR-2].	SysC-2
	· **UCA-3:** The control room operator swung open the furnace roof while the electrode was below its pass line and not clear of the roof. [SR-1].	SysC-3
	· **UCA-4:** The control room operator moved the electrode without having a visual reference to validate its precise position. [SR-2].	-
	· **UCA-5:** Plant operators restarted operations without performing a pre-startup safety review (PSSR) to check operational readiness, including systems, equipment integrity, and organizational factors. [SR-2, SR-3].	-
	· **UCA-6:** Plant operators restarted operations without PLC safety protections in place. [SR-3].	-
Process Model and Mental Flaws	· **PM-1:** The control room operator believed the electrode was not hooked to the crane. [UCA-1].	-
	· **PM-2:** The crane operator believed the operator in the control room knew the electrode was hooked to the crane. [UCA-1].	HC-1
	· **PM-3:** Operators believed the recurrent failure in the electrode's position system could be tolerated and was not a potential cause of accidents. [UCA-2].	-
	· **PM-4:** The control room operator believed the pass line of the furnace roof was clear without interferences. [UCA-3].	-
	· **PM-5:** Operators knew that designed safety protections were not activated, but they believed that it was safe to continue the start-up. [UCA-4, UCA-6].	-
	· **PM-6:** Plant operators believed one of the goals of the start-up was to test the new features of the PLC, so finding inactive safety protections were not unusual. [UCA-6].	-
Context	· **C-1:** The control room operator and the crane operator coordinate tasks through radiofrequency. The supervisor directly told to the crane operator to hook the electrode without informing the control room operator over the radio. [PM-1, PM-2].	-
	· **C-2:** As the plant was in its start-up process, the communication radio channels were busy, making it hard to understand and follow instructions. [PM-1, PM-2].	-
	· **C-3:** The operators developed a nonstandard practice to deal with the recurrent failures of the electrode's positioning system. [PM-1].	-
	· **C-4:** The standard procedures were not revised to address the deficiencies of the system that the control room operators uncovered. [PM-1].	-
	· **C-5:** During the plant start-up, several failures in the automatic sequences and protections occurred. For example, one of the protections in the former PLC disabled the movement of the furnace roof if the mast was not at its top position. This protection was not configured in the new PLC used to restart the plant operations. [PM-1, PM-5].	-
	· **C-6:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. While they believed that not having the safety protections was tolerable, this perception may have shaped by the pressure they were facing due to the shutdown delay. [PM-5, PM-6].	-

	· **C-7:** During the shutdown, the control room was moved to another location (farther away from the furnace). Additionally, all the HMIs were replaced by new standardized interfaces. The visual reference the operators used to have (tape on glass) to determine the position of the electrode was not present in the new location. [PM-4].	-
	· **C-8:** Both the control room operator and the crane operator were relatively new in their positions (less than six months). [UCA-5].	-
	·**C-9:** The pressure to restart production was higher than the pressure to stop production if a non-relevant safety issue was discovered. [PM-5].	-
Operations Engineers and Supervisors		
Unsafe decisions and control actions	· **UCA-1:** The supervisor requested the crane operator to hook the electrode without informing the control room operator. [SR-1].	-
	· **UCA-2:** Did not request the operators to perform a pre-startup safety review (PSSR) to check operational readiness, including systems, equipment integrity, and organizational factors. [SR-2, SR-3, SR-8].	-
	· **UCA-3:** Approved to restart production without safety protections in place. [SR-3, SR-8].	-
	· **UCA-4** Did not assess potential risks associated with substandard and nonstandard operations and did not provide corrective actions. For example, the nonstandard procedure used to deal with the electrode's positioning issue. This practice was not revised and properly documented. [SR-3, SR-5].	SysC-2
	· **UCA-5:** Did not assess potential shortcomings related with the changes in the plant (e.g., the loss of visual reference to validate the electrode's position due to the relocation of the main control room, or the modification of the piping length over the furnace roof). [SR-8].	PC-1
	· **UCA-6:** Developed safety procedures inadequately detailed to manage an emergency due to a severe water leak. [SR-4].	-
Process Model and Mental Flaws	· **PM-1:** The supervisor believed the control room operator had noticed that the crane operator hooked the electrode. [UCA-1].	HC-1
	· **PM-2:** The supervisor believed the mast stopped because it reached its maximum position or at least reached a sufficient height to continue the operation. [UCA-1].	-
	· **PM-3:** The supervisor may have believed that since the mast had stopped, the control room operator had stopped the motion and was now waiting for the crane to hook the electrode. [UCA-1].	-
	· **PM-4**: The operations engineer and supervisors may have believed the PSSR was not relevant as the organization did not require it. [UCA-2].	-
	· **PM-5:** The operations engineer and supervisors agreed to continue the plant start-up despite the safety protections in the PLC to control the position of furnace components were not activated. They believed it was safe to continue the start-up under this condition. [UCA-3].	-
	· **PM-6:** They believed the nonstandard workaround to deal with the failures in the electrode's position system was only a temporary measure and not a potential cause of accidents. [UCA-4].	-
	· **PM-7:** They believed the relocation of the control room would not have impacts in the plant operations. [UCA-5].	-

	· **PM-8:** The engineers and supervisors believed the procedure that described the process to follow in case of an emergency due to a water leak was good enough to control the emergency. [UCA-6].	-
Context	· **C-1:** The control room operator and the crane operator coordinated tasks through radiofrequency. The supervisor directly told the crane operator to hook the electrode without informing the control room operator by radio. The crane operator failed notify the control room operator that the electrode was hooked. [PM-1].	-
	· **C-2:** The PSSR was not a common practice in the organization. A formal procedure did not exist to perform it. The operations team conducted a mental check based on the expertise of the operators, supervisors, and engineers to validate the readiness of the facility to start operations. [PM-4].	-
	· **C-3:** For the organization, having problems during the plant start-up was not an ideal situation, but it was considered part of the process. The supervisors acknowledged it and decided that it was feasible to continue the start-up but demanding more attention and coordination from the operators to ensure ta safety start-up. [PM-5].	-
	· **C-4:** The PLC to control the position of furnace elements was in a critical condition due to its saturation and obsolescence. The engineering team had planned to replace it by a new model during the shutdown. Therefore, while the engineers and supervisors recognized that workarounds were not ideal, the risk to repair the PLC to solve the electrode's positioning problem could be problematic. So, they decided to wait for the replacement of the PLC and considered the nonstandard practice as an effective and safe temporary solution. [PM-6].	-
	· **C-5:** During the shutdown, the control room was moved to another location (farther away of the furnace), and a new standardized interface replaced the previous HMIs. The visual reference the operators used to have (tape on glass) to determine the position of the electrode was lost. [PM-7].	-
	· **C-6:** No similar incidents had occurred in the Fuchs furnace in recent years. Therefore, the engineers and supervisors did not think about different failure scenarios while documenting the procedure to control water leaks. [PM-6].	-
	· **C-7:** The pressure to restart production was higher than the pressure to stop production if a non-relevant safety issue was discovered. [PM-5].	-
Operations Management		
Unsafe decisions and control actions	· **UCA -1:** Managers did not define as a standard requirement the performance of pre-startup safety review (PSSR) to check operational readiness, including systems, equipment integrity, and organizational factors. [SR-2, SR-3, SR-8].	-
	· **UCA-2:** The management approved to continue the plant start-up despite the flaws in the automation to control the position of the furnace components (e.g., safety protections disabled). [SR-3, SR-8].	-
	· **UCA-3:** The operations management did not establish a policy for the management of change to identify, manage, and control modifications to standard procedures or operational thresholds. For example, the nonstandard practice to deal with the electrode's positioning issue was not properly analyzed and documented. [SR-1, SR-2, SR-3, SR-5].	-

	· **UCA-4:** The operations management did not proactively expand the hazard analysis from previous events to the Fuchs furnace. A similar incident previously occurred in the Danieli EAF. However, the analysis and lessons learned were not extrapolated to the Fuchs EAF (e.g., the need of an automatic system to control the cooling system remotely, the need of sensors to monitor the status of the cooling system). [SR-10].	PC-3
	· **UCA-5:** The operations management team did not prioritize the capital expenditures (CAPEX) according to formal risk evaluations. The investment plan priorities were defined according to the expertise, judgment, and requirements of the management. [SR-11].	-
	· **UCA-6:** The management approved standard procedures inadequately detailed to perform critical tasks (e.g., what to do in case of a severe water leak). [SR-4, SR-5].	-
	· **UCA-7:** The management did not request and validate the risk assessments before the execution of projects and modifications that were implemented during the shutdown. [SR-8].	-
	· **UCA-8:** Underestimated the impacts of the modifications in the control room (change of location of the control room and change of HMIs). [UCA-12].	PC-1
Process Model and Mental Flaws	· **PM-1:** The management may have believed the PSSR was not required since the operations team had enough experience in plant start-ups after maintenance shutdowns. [UCA-1].	-
	· **PM-2:** They believed one of the goals of the start-up was to test the new features of the PLC and the new equipment, so problems were expected (e.g., inactive safety protections may have been not unusual). [UCA-2].	-
	· **PM-3:** The operations management believed any relevant safety issues discovered during startup would be reported and reviewed by engineers and supervisors. [UCA-2].	-
	· **PM-4:** They believed the management of change policy was necessary to control the constant changes and modifications in the plant. [UCA-3].	-
	· **PM-5:** Management may have believed that the opportunity areas found in recent safety events were more related to isolated human errors or negligence rather than systemic factors. [UCA-4].	-
	· **PM-6:** The management may have believed that the safety needs in the plant were obvious. Thus, no formal analysis was required to determine the priorities regarding safety for the CAPEX plan. [UCA-5].	-
	· **PM-7:** The management believed the engineers and supervisor had developed detailed procedures. Therefore, they may have approved them without performing a meaningful check. [UCA-6].	-
	· **PM-8:** The management believed the best option was to open the furnace roof since the water was getting into the furnace, even though this situation was not documented. [UCA-6].	-
	· **PM-9:** The management may have believed that the risk assessments traditionally performed by the engineering team should be good enough to cover all the safety aspects. Therefore, they may not have exhaustively reviewed them to detect potential flaws. [UCA-7].	-
	· **PM-10:** The management believed that the relocation of the control room would not be a problem for the operators. They did not consider the requirement to have a reference to validate the position	-

	of the electrode, as the operator used to have a tape on the glass of the control room. [UCA-8].	
Context	· **C-1:** The PSSR was not a common practice in the organization. Normally, a mental check was performed previous or during the start-up process. [PM-1].	-
	· **C-2:** For the management, having problems during the plant start-up was part of the process. They believed it was a good opportunity to test the new equipment to identify flaws in the design or during the installation. Therefore, problems were expected and considered in the start-up of the plant. [PM-2, PM-3].	-
	· **C-3:** The management realized that a management of change policy was needed to control the continuous changes the organization faced. However, they had not achieved this purpose to set a standard mechanism to manage the change. [PM-4].	-
	· **C-4:** The analysis of the safety events was focused more on physical and human factors, rather than systemic causes. This approach did not provide the envision to the company to understand the dynamics of events as a whole. Therefore, the causes were isolated and not extrapolated to other situations. [PM-5].	-
	· **C-5:** The company did not have a formal process to prioritize investments according to risk assessments. Traditionally the prioritized projects were the ones related to high-risk safety events that had occurred in the company. [PM-6].	-
	· **C-6:** All procedures, depending on the relevance, had to be approved at different levels of management. Managers were overwhelmed. Thus, like normal, they did not have the time to review in detail the procedures. [PM-7].	-
	· **C-7:** When the water leak occurred, the plant manager realized that the amount of water getting into the furnace was significant. Thus, he decided that the furnace roof needed to be open in preparation for an imminent explosion. If an explosive reaction happened with the furnace closed, the damages to the furnace and to its surroundings, including people might have been worst. [PM-8].	-
	· **C-8:** The engineering team typically performed risk assessments before the execution of projects. However, they were not rigorous and detailed in the assessment of the possible impacts the projects could have. [PM-9].	-
	· **C-9:** When the main control room was relocated, the visual reference used to validate the position of the electrode was lost. [PM-10].	-
Maintenance Technicians and Contractors		
Unsafe decisions and control	· **UCA-1:** The maintenance technicians did not evaluate and informed to their superiors the risks that the modification in the piping over the roof could cause. [SR-4, SR-5].	-
	· **UCA-2:** They did not verify that the evacuation emergency siren was operating before starting the plant start-up. [SR-6].	-
Process Model and Mental	· **PM-1:** The maintenance technicians believed the piping modification was only a minor change that would not have a negative impact on safety. The technicians thought the modification would indirectly improve safety as it could facilitate the repair in case of a water leak. [UCA-1].	-

	· **PM-2:** They believed the start-up of the plant was an opportunity to test and validate the modifications made during the shutdown. [UCA-1].	-
	· **PM-3:** The maintenance technician believed the emergency siren was going to be reconnected by the engineering team since they were conducting the control room revamping project. [UCA-2].	-
Context	· **C-1:** In the past, minor modifications to equipment were executed without proper documentation and hazard assessments. It was not adequately stated what kinds of modifications required documentation, and who was responsible for this activity. [PM-1].	-
	· **C-2:** The shutdown had an extensive scope, and many types of equipment were intervened to perform preventive or corrective maintenance. The plant start-ups have traditionally been the opportunity for the maintenance team to verify the condition of the equipment after the maintenance. [PM-2].	-
	· **C-3:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. [PM-2].	-
	· **C-4:** The maintenance technicians were not aware of all details of the modifications the engineering team was conducting during the shutdown. In normal operations, the maintenance technicians were responsible to keep all alarms in operation, but as the control room revamping project was out of their scope, they did not ensure the emergency alarms were in place. [PM-3].	-
Maintenance Leaders and Supervisors		
Unsafe decisions and control actions	· **UCA-1:** The maintenance leaders and supervisors agreed to restart operations without performing a pre-startup safety review (PSSR) to check operational readiness, including systems and equipment integrity. [SR-2, SR-3, SR-8, SR-9].	-
	· **UCA-2:** The maintenance leaders did not perform a meaningful risk assessment of the modification on the piping length over the furnace roof to identify potential risks. [SR-8, SR-9].	-
Process Model and Mental Flaws	· **PM-1:** They believed a formal PSSR was not required as the start-up process was typically the time to test and verify the condition of the equipment. [UCA-1].	-
	· **PM-2:** They believed the piping modification was only a minor change that would not have a negative impact on safety. The maintenance team thought the modification would improve safety as it could facilitate its overhaul in case of a water leak. [UCA-2].	-
Context	· **C-1:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. A complete PSSR may have delayed more time the beginning of the plant start-up. [PM-1].	-
	· **C-2:** A formal PSSR was not a requirement in the organization. However, the maintenance leaders and supervisors supported the operations teams through the mental check they performed before the start-up. This verification relied on the expertise primarily of the maintenance leaders and supervisors, as well the operations engineers and supervisors. [PM-1].	-
	· **C-3:** The maintenance team did not have a robust policy for management of change. It was not clear what kind of modifications required documentation, and who was responsible for this activity. The maintenance leaders considered the modification of the roof piping as an improvement, but they did not perform a study to evaluate the potential shortcomings of this modification. [PM-2].	-

Maintenance Management		
Unsafe decisions and control actions	· **UCA-1:** The maintenance management did not request the performance of a pre-startup safety review (PSSR) to check operational readiness, including systems and equipment integrity. [SR-2, SR-3, SR-8, SR-11].	-
	· **UCA-2:** The maintenance management did not proactively extrapolate the analysis of similar events to the Fuchs furnace. [SR-10].	-
	· **UCA-3:** The maintenance management may not have considered as a top priority the instrumentation of the cooling system, neither the need for an automatic system to control it remotely. [SR-11].	PC-3
	· **UCA-4:** The maintenance management did not request the performance of risk assessments for the modifications implemented during the shutdown. [SR-8, SR-12].	-
Process Model and Mental Flaws	· **PM-1:** The maintenance management believed the PSSR was not necessary as the start-up was the opportunity to test all equipment and the modifications implemented during the shutdown. [UCA-1].	-
	· **PM-2:** The maintenance management may have believed that the causes identified in previous safety events were isolated, and not applicable to the Fuchs furnace. [UCA-2].	-
	· **PM-3:** They may have believed that as there were no records of high-risk incidents related to water leaks, the needs of instrumentation or to automate the controlling valves were not as important as other priorities. [UCA-3].	-
	· **PM-4:** They may have believed that the modifications implemented during the shutdown were irrelevant concerning safety (e.g., the piping modification in the furnace roof), so no safety assessment was needed. [UCA-4].	-
Context	· **C-1:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. [PM-1].	-
	· **C-2**: The PSSR was not standard procedure in the organization. While the organization had discussed the convenience to implement it, it was not a requirement. [PM-1].	-
	· **C-3:** The analysis of safety events was focused more on physical and human causes, rather than systemic factors. This situation inhibited the extrapolation of lessons learned from past events to have a proactive call to action. [PM-2].	-
	· **C-4:** No high-risk incidents were recorded in the Fuchs related to water leaks. Thus, no red flags were rose regarding the cooling system at that time. [PM-3].	-
	· **C-5:** The organization did not have a specification to define what was a minor modification, as well as if it required a risk assessment before its implementation. The maintenance management did not encourage the following of a policy for management of change. [PM-4].	-
Engineering Worker		
Unsafe decisions and control	· **UCA-1:** The engineering workers agreed to begin the start-up process without ensuring the safety protections of the new PLC were enabled. [SR-2, SR-3, SR-8].	-
	· **UCA-2:** The engineering workers did not perform extensive testing to detect potential flaws in the modifications implemented prior to their start-up. [SR-8].	-

	· **UCA-3:** The engineering workers did not enable the safety protections in the new PLC to control the position of the furnace components. [SR-8].	-
	· **UCA-4:** The engineering workers did not consider the requirement from operators to have a reference to validate the position of the lower end of the electrode. [SR-8].	PC-1
	· **UCA-5:** The engineering workers did not perform meaningful risk assessments to cover the possible failure scenarios for the both modifications and the newly implemented equipment. [SR-8].	-
	· **UCA-6:** The engineering workers did not connect the evacuation emergency alarm in the new control room. [SR-4].	-
Process Model and Mental Flaws	· **PM-1:** The engineering workers realized that the safety protections were not activated when the start-up began, but they believed that it was safe to continue as the operations team had approved. [UCA-1].	-
	· **PM-2:** They believed one of the goals of the start-up was to test the new features of the PLC, so finding inactive safety protections were not unusual. [UCA-1].	-
	· **PM-3:** The engineering workers may have believed that performing trials before the start-up could disturb or affect the normal operations. [UCA-2].	-
	· **PM-4:** The engineering workers unintentionally omitted the enable of the safety protections of the new PLC. They believed the protections were in place at the beginning of the start-up. [UCA-3].	-
	· **PM-5:** The engineering workers may have believed that the requirement to have a visual reference was not relevant since the control room operator already had a position reference coming from the mast's encoder. [UCA-4].	-
	· **PM-6:** They believed the risks assessments developed were good enough to prevent the failure scenarios they have considered as possible. [UCA-5].	-
	· **PM-7:** They may have believed the evacuation emergency alarm was in place. [UCA-6].	-
Context	· **C-1:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. The operations teams agreed to continue the start-up as it was the opportunity to detect more potential flaws or problems. [PM-1].	-
	· **C-2:** After extensive maintenance shutdowns, failures normally occurred, thus the organization accepted as normal to have problems during the start-up. The former PLC to control the furnace positions used to have restrictions to avoid collisions between movable components (e.g., between the electrode and the furnace roof). However, during the start-up, the new PLC did not perform these restrictions due to the engineering workers disabling them. [PM-2].	-
	· **C-3:** The Fuchs furnace was one of the main production lines in the company. However, the engineering workers determine that it was not convenient to perform a test prior to the shutdown due to the critical condition of the PLC and the risks that it may imply. [PM-3].	-
	· **C-4:** The engineering workers may not have had a robust verification process prior to the start-up of new equipment. They discovered the protections were not in place when the control room operator informed that he could move the furnace roof even though that the mast was not at its top position. [PM-4, PM-6].	-

	· **C-5:** The engineering workers did not address the need to have a reference to validate the position of the electrode as they did not get the requirement from the operations team. [PM-5].	-
	· **C-6:** At that time, robust engineering hazard assessments were not mandatory performed before the project execution. The hazard assessments that were in used did not provide a reliable way to detect missing or incorrect requirements. [PM-2, PM-3, PM-5, PM-6].	-
Project Manager		
Unsafe decisions and control actions	· **UCA-1:** The project manager did not define an effective mechanism to validate the performance of modifications, as well as the newly added equipment was according to design. [SR-4, SR-8, SR-11].	-
	· **UCA-2:** The project manager approved the design and location of the new control room without ensuring all needs from the operations team were covered. [SR-8].	PC-1
	· **UCA-3:** The project manager may not have spent enough time to review that the risk assessments of the projects were meaningful. [SR-8].	-
Process Model and Mental Flaws	· **PM-1:** The project manager believed that the plant start-up was a good opportunity to detect the flaws in design or errors during the implementation of projects. [UCA-1].	-
	· **PM-2:** The project manager believed that conduct trial tests prior to the shutdown could be dangerous as the condition of the former PLC was critical due to its obsolescence. [UCA-1].	-
	· **PM-3:** The project manager believed they had collected all the requirements from the operations teams regarding the new control room. [UCA-2].	-
	· **PM-4:** They project manager believed the risk assessments performed by the engineering workers were enough to prevent most of the possible failure scenarios. [UCA-3].	-
Context	· **C-1:** The organization was under pressure to restart operations since the maintenance shutdown was behind schedule. As time was constrained, the time to test the modifications was shortened. Thus, the tests were conducted during the start-up. [PM-1].	-
	· **C-2:** The condition of the former PLC to control the position of the furnace components was critical, so the engineering team, together with operations and maintenance, decided to wait for the shutdown to replace it. Therefore, there was no opportunity to perform tests before its implementation. [PM-2].	-
	· **C-3:** The process to collect the requirements from operations or maintenance was not robust. Typically, the operative areas were overwhelmed with their daily activities, so they spent insufficient time to review the projects. However, the project manager tried to collect as much of the information as possible to develop the project. [PM-3].	-
	· **C-4:** The project manager was overwhelmed with activities; thus, he may have had no time to check the risk assessments carefully. [PM-4].	-
Engineering Management		
Unsafe decisions and control	· **UCA-1:** The engineering management did not request to have a robust procedure to detect early flaws in projects. [SR-8, SR-12].	-
	· **UCA-2:** The engineering management did not request to perform robust engineering hazard assessments to prevent potential accidents. [SR-8].	-

	· **UCA-3:** The engineering management did not extrapolate the lessons learned from past safety events to prevent future accidents. [SR-9].	PC-3
	· **UCA-4:** The engineering management allocated CAPEX resources without performing a risk analysis to prioritize projects. [SR-10].	-
Process Model and Mental Flaws	· **PM-1:** The engineering management may have believed the reviews performed by the project managers and engineering workers were enough to prevent mishaps. [UCA-1].	-
	· **PM-2:** The engineering management may have believed that the risk assessments conducted by the project manager were good enough. [UCA-2].	-
	· **PM-3:** They may have believed that the causes of previous events were isolated human errors or negligence rather than systemic factors. [UCA-3].	-
	· **PM-4:** The engineering management may have believed that it was not necessary to perform a risk analysis to identify the investment priorities. [UCA-4].	-
Context	· **C-1:** The engineering team was overwhelmed with duties. A more robust procedure to validate the project designs would have implied more effort from the project managers and engineering workers. Thus, the management considered the process at that time were good enough to prevent potential flaws and accidents. [PM-1].	-
	· **C-2:** Similarly, more robust safety assessments would have demanded more time from an organization that was already overloaded with activities. The management may have considered that the assessments performed had a good trade-off between the effort and quality and that they were sufficient to detect and prevent safety anomalies. [PM-2].	-
	· **C-3:** A similar incident previously occurred in the Danieli furnace. The analysis, besides other aspects, recommended the instrumentation of the cooling system to monitor it actively. Additionally, the analysis recommended the installation of automated valves to shut-off the system in case of an emergency. Those recommendations also applied to the Fuchs furnace. However, other projects were prioritized over these needs. [PM-3].	-
	· **C-4:** The organization did not have a formal process to prioritize the CAPEX for safety projects. Therefore, the allocation of resources was influenced by high-risk accidents that had occurred recently. Additionally, the benefits of safety investments were hard to be translated into economic terms. Thus, they may not have seen as attractive as other projects related to performance improvement. [PM-4].	-
Safety Engineer		
Unsafe decisions and control actions	· **UCA-1:** The safety engineer did not promote the pre-startup safety review (PSSR) to be a mandatory procedure to be performed prior to the start-ups. [SR-2, SR-3, SR-4, SR-5].	-
	· **UCA-2:** The safety engineer did not assess the risks to perform nonstandard practices to deal with substandard conditions (for example, the workaround to deal with the electrode's positioning issue). [SR-1, SR-2, SR-3, SR-5].	-
	· **UCA-3:** The safety engineer did not detail the emergency procedures to control water leaks. [SR-4].	-

	· **UCA-4:** The safety engineer may not have followed up the lessons learned and action plans from previous similar events to apply them to other production lines. [SR-10].	PC-3
	· **UCA-5:** The safety engineer did not actively participate during the design and planning phase of the shutdown to detect the potential hazards related to the engineering or maintenance modifications. [SR-11].	-
	· **UCA-6:** The safety engineer did not develop a meaningful risk assessment of the projects and modifications implemented during the shutdown. [SR-5].	-
Process Model and Mental Flaws	· **PM-1:** While the safety engineer believed the PSSR was a relevant procedure to manage the risks during a start-up, he believed it would require first the approval from the operations management. [UCA-1].	-
	· **PM-2:** The safety engineer believed the workaround to deal with the electrode's positioning issue would not represent a safety issue. [UCA-2].	-
	· **PM-3:** The safety engineer believed the emergency procedure to control the water leaks was adequate. It had been active for a long time and had been reviewed and approved by the management. [UCA-3].	-
	· **PM-4:** The safety engineer may have believed that lessons learned from similar past events were considered in an improvement plan for the Fuchs furnace. [UCA-4].	-
	· **PM-5:** The safety engineer may have believed that his participation during the design and planning phases of projects was not relevant, as typically the engineering team performed the safety assessments on their own. [UCA-5, UCA-6].	-
Context	· **C-1:** The operations team may not have been convinced about the need to have a specific procedure to check the readiness of the plant prior to its start-up. The safety engineer acknowledged this situation, and as the operations team had never performed this procedure and there was no record about high-risk incidents related to this topic, the safety engineer did not insist on its relevance. [PM-1].	-
	· **C-2:** The workaround to deal with the electrode's positioning issue became a normal practice for the operators. As it was performed recurrently without no relevant issues, over time, it created a false sense of security within the operations team and safety team. It was considered as a temporary solution which was planned to be solved during the shutdown. However, although the former PLC was replaced in the shutdown, the issue manifested during the start-up as the operations and engineering team did not properly address it. [PM-2].	-
	· **C-3:** The emergency procedure that described what to do in case of a water leak, had been reviewed and approved by the operations management. However, it did not include different failure scenarios, including what do in case of a severe water leak in the furnace roof. The fact that the management reviewed the procedure created false confidence that the procedure was complete. [PM-3].	-
	· **C-4:** The lesson learned and recommendations from the incident in the Danieli furnace were shared to different levels and teams in the organization. The deficiencies on the cooling system of the Danieli furnace, regarding its monitoring and control, were prompt addresses by the organization. However, they were not addressed with the	-

	same sense of urgency on the Fuchs furnace, although the risk level was similar on both production lines. [PM-4].	
	·**C-5:** The safety engineer was coped with activities concerning occupational safety tasks rather than process safety. The safety structure was very lean, having only one engineer for the steelmaking process. He did not have sufficient time to participate in the engineering and safety assessments performed by the engineering team. [PM-5].	-
Safety Management		
Unsafe decisions and control actions	· **UCA-1:** The safety management did not request the pre-startup safety review (PSSR) to be a mandatory procedure to be performed prior to the start-ups. [SR-2, SR-3].	-
	· **UCA-2:** The safety management did not promote that the action plans from past events were expanded to other facilities with similar issues. [SR-7].	-
	· **UCA-3:** The safety management did not define a robust policy of management of change to control the modifications adequately on facilities. [SR-10].	-
	· **UCA-4:** The safety management may not have promoted the prioritization of CAPEX according to risk evaluations. [SR-8].	-
	· **UCA-5:** The safety management did not define as a requirement the performance of robust engineering and safety assessments prior to the implementation of projects. [SR-10].	-
	· **UCA-6:** The safety management may not have encouraged the active participation of the safety team during the design and planning phases of projects and shutdowns. [SR-9].	-
	· **UCA-7:** The safety management did not establish the use of more comprehensive methods to analyze and prevent accidents. [SR-10].	-
Process Model and Mental Flaws	· **PM-1:** While the safety management believed the PSSR could be a helpful tool to manage the risks during a start-up, they believed it required the buy-in from the operations management to be effective. [UCA-1].	-
	· **PM-2:** The safety management team believed the lesson learned and actions defined for previous events were known by the operations, maintenance, and engineering teams. [UCA-2].	-
	· **PM-3:** The safety management believed the management of change should be an important milestone in the safety management of the organization. But, they did not define how to achieve this goal. [UCA-3].	-
	· **PM-**4: The safety management may have believed that the operations and engineering team controlled the CAPEX and that they did not have strong leverage to make recommendations. [UCA-4].	-
	· **PM-5:** The safety management may have believed the assessments prepared by the safety engineers and the engineering team prior to the implementation of projects was good enough to prevent accidents. [UCA-5].	-
	· **PM-6:** The safety management believed the safety engineers were deeply involved in the planning of projects and shutdowns. [UCA-6].	-
	· **PM-7:** The safety management believed that the safety methods they were using (e.g. RCA) were good enough to understand the causality of the events. [UCA-7].	-

Context	· **C-1:** The idea to implement the PSSR after extensive shutdowns had been under the analysis of the organization for a long time. However, the organization may not have been fully convinced about the benefits that this practice could bring. The safety management did not push forward this plan. Instead, they focused on other aspects that they believed could have more impact on the safety performance of the company (e.g., identify and classify the activities performed by the operators according to their risk). [PM-1].	-
	· **C-2:** The safety management may have considered that the analyses from past events were shared and available to the organizations. Therefore, the operations, maintenance, and engineering teams knew what the recommendations were, and which could apply to the Fuchs furnace as well. However, the safety management may not actively have promoted the inclusion of the Fuchs furnace on the plan to solve the deficiencies of the cooling system of the other furnace. [PM-2].	-
	· **C-3:** Management of change had been a topic that concerns the organization. However, safety management had not defined how to address this milestone to control the continuous changes in the process, systems, and equipment. For example, the modification of the piping length of the furnace roof was not followed by a risk assessment to address the potential impact of this modification. [PM-3].	-
	· **C-4:** The safety management should have been a compass to guide the organization where to allocate the resources to improve the safety performance of the company. However, safety may not have played a significant role in the definition of the CAPEX of the organization. The definition of priorities was defined normally by the operations and engineering team. Thus, the prioritization could have had a bias towards other priorities such as productivity and economic returns. [PM-4].	-
	· **C-5:** The safety management may have not had the time to review in detail the safety assessments developed by the safety engineers or the engineering team. Therefore, they would feel confident about the completeness of the assessments performed by them. [PM-5].	-
	· **C-6:** The safety engineers normally participated in some meetings for shutdown planning. However, they did not get into details about the specifications of the modifications to validate if those modifications could increase the risk factors since they had other responsibilities. Similarly, the safety engineer participated briefly in the design phase. [PM-6].	-
	· **C-7:** RCA has been the standard method to analyze accidents by the organization for several years. While the approach could be helpful to determine the causes of an accident, it has considerable limitations to understand the full dynamic of events in complex systems and large organizations. [PM-7].	-
Corporate Management		
Unsafe decisions and control	· **UCA-1:** Did not require in-depth analysis of incidents and accidents that rigorously considered and emphasized systemic causes. [SR-10].	-
	· **UCA-2:** The corporate management may not have allocated enough resources for implementing corrective actions broadly throughout other units. [SR-4, SR-8].	-

	· **UCA-3:** Did not require robust engineering and safety assessments prior the CAPEX approval. [SR-4].	-
	· **UCA-4**: May did not have adequately fostered a safety culture in the organization in which safety was prioritized over other goals. [SR-2].	-
Process Model and Mental Flaws	· **PM-1:** Believed recent safety events were more related to isolated human errors or negligence than systemic factors. [UCA-1].	-
	· **PM-2:** Believed the analysis performed by the engineering team to support the CAPEX request were adequate. [UCA-3].	-
	· **PM-3:** Believed the organization was clear about safety was the priority and that their actions were aligned to this goal. [UCA-4].	-
Context	· **C-1:** The analyses of incidents and accidents were performed following a Root Cause Analysis method focusing more on physical (e.g., equipment failures) and human causes, rather than systemic causes. Similar incidents occurred previous to this event, but the lessons learned, and the action plans defined were not implemented in the Fuchs with a sense of urgency as in the Danieli furnace. Although both facilities had similar risk levels. [PM-1].	-
	· **C-2:** The CAPEX requests had to include an engineering and safety assessment and had to pass through an extensive channel of approvals from different management levels. By the time the requests had reached the upper management, they have been reviewed by several people from different areas and hierarchical levels. Therefore, corporate management may have felt confident that the project was well supported and prioritized regarding safety. [PM-2].	-
	· **C-3:** Management may have felt confident that the organization was engaged towards safety due to good results in the overall safety indicators of the company. However, they may not have had the right pulse of what was happening at the floor level, seeing if the people believed that safety was the main priority for the organization. [PM-3].	-

5.2 Analysis of Results

Tables 25 and 26 shown the contrast of the outcomes between CAST and RCA. All the causes and factors identified in the RCA analysis were addressed by CAST. CAST provided a comprehensive lists of factors which enable the organizations to understand what were the reasons behind the causality of the event.

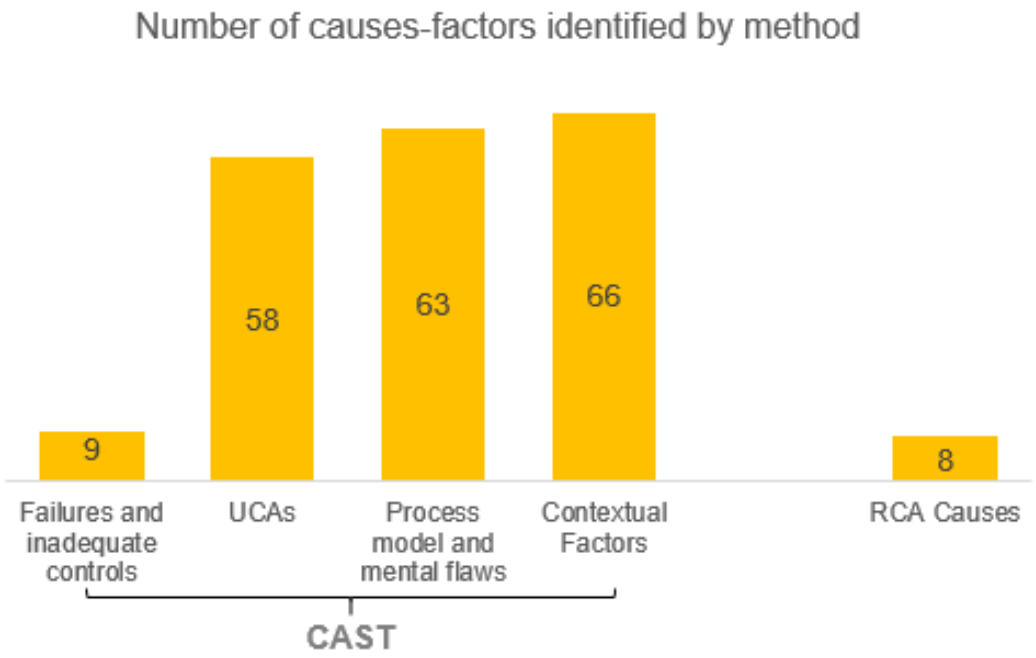


Figure 36: Graphic representation of number of causes and factors detected by model

More importantly, than the per se number of causes is the quality of the detected causes. The CAST analysis accounted several factors that were not addressed by the RCA analysis. Some of the principal causes that were not pinpointed in the RCA analysis, and are relevant to comprehend why the incident occurred are listed below:

- *The performance of inadequately detailed risk assessment to prevent and mitigate possible failure scenarios in projects and modifications.*

  The organization had as standard the performance of engineering hazard assessments prior to the execution of projects. However, the robustness of these analyses may not have been enough to determine the potential failures the project could experience. To have a meaningful assessment to cover most of the possibilities of failure, the engagement from the users and other stakeholders is fundamental as they have the expertise on the field and may provide relevant information to consider while designing a project.

- *The absence of a formal pre-start safety reviews process to ensure the readiness of the plants before their start-up.*

  The plant did not have a checklist to validate the condition of critical equipment and to detect if critical control systems operate correctly. For example, the emergency sirens

were out of service, thus when the first reaction occurred, the signal to evacuate was communicated via radiofrequency. However, at that moment, not all the personnel carried a portable radio to receive this notification.

On the other hand, during the start-up, some of the automatic sequences and protections of the furnace were not available or were not performing adequately due to the revamp made to the process controllers. For example, the protection to halt the roof swinging if the electrode was not at its top position, was deactivated during the start-up. However, the organization decided to continue the restarting process believing those flaws could be addressed later while running the plant.

Besides, the PSSR could be an effective procedure to diagnose the require workforce to perform the plant start-up. For example, qualified operators and supervisors with sufficient expertise on plant start-ups are critical factors in achieving a successful performance.

- *The lack of a robust policy for management of change to validate and control the modifications performed within the organization.*
  This topic is particularly important in organizations that are experiencing constant changes. An adequate control process will ensure that each change and modification is adequately defined, assess the risks implied, and get the approval from the management. In this case study, several modifications took place during the shutdown that were not adequately analyzed to identify its potential shortcomings. For example, the modification of the length of the piping of the furnace roof that increased the risk of being damaged. Also, the modification of the main control room which did not consider the need to have a visual reference for the operators to validate the electrode's position.

- *The lack of risk analysis to support the prioritization of the CAPEX allocation.*
  The benefits from investments in safety tend to emerge only in the long run and may only be indirectly observable as non-accidents or the avoidance of modifications or retrofits to improve safety [3]. In the end, a prudent operation strategy regarding safety will be more sustainable in the future than a strategy based on short-term benefits.

- *The decision to restart operations knowing the safety flaws in systems (e.g. PLC safety protections disabled, issues with the electrode's positioning).*

  The organization defined that as the plant was during its restarting process, this inconvenient of not having available the safety protections of the PLC for furnace motions PLC was not a major issue. This situation was considered as tolerable, there was no policy or procedure to prevent startup in this situation, and the operations team decided to go on with the startup.

  While the operations team defined that it was possible to continue the startup process of the plant, it is necessary to understand why the new PLC did not perform as expected regarding safety. The organization needs to define procedures and control mechanism to ensure that new equipment and modifications performed as expected. Safety should be controlled by design. To achieve this, it is necessary to perform a preventive analysis to capture possible unsafe actions and failure scenarios. The following chapter of this thesis demonstrates how STPA could be helpful to uncover possible modes of failure and prevent accidents.

- *The lack of a comprehensive method to analyze incidents and accidents that rigorously considered and emphasized systemic causes.*

  The method used by the organization to analyze incidents and accidents did not have a systemic approach. The RCA analysis normally focused more in human and physical factors; therefore, the typical outcome of investigations was that some equipment needed to be replaced or to be updated, and that the operators needed to be re-train to ensure the procedure compliance.

  Traditionally, a few or no systemic causes were identified in the investigation of safety events in the organization. The lack of systemic causes was a lost opportunity to detect the real underlying factors of those accidents and to prevent future events.

Chapter 6: Could these type of accidents be prevented?

The CAST analysis provided a comprehensive list of weaknesses throughout the control structure and at different organizational levels that led to the incident. The analysis suggested a set of recommendations to correct these issues and avoid similar events in the future. Since CAST has a holistic perspective, the suggested recommendations aim to address not only low-level aspects like component failures and operator actions involved in one specific incident but systemic factors that contribute more generally to this and many other types of incidents.

However, learning through incidents is not the most effective and reasonable strategy to improve. Why weren't these factors identified and corrected before the incident occurred? Careful reviews and hazard analyses had been performed to anticipate what could go wrong before the incident, but they were not effective in preventing this incident and they did not anticipate the full set of weaknesses and causes identified by CAST.

Systems Theoretic Process Analysis, STPA, is a hazard technique based on the same principles as CAST but it is applied before an accident occurs to proactively identify and correct weaknesses throughout the system. STPA anticipates unacceptable losses by modeling the safety control structure, identifying unsafe control actions, and creating potential loss scenarios.

This chapter identifies the improper or missing controls that allowed the Fuchs EAF system to migrate to a higher risk level. At the end of the chapter, insights are presented about the difficulty of applying this technique for people who are not familiar with it. This experiment provides intuition about the acceptability from users and the possibility to adopt this technique as a reference to prevent undesirable safety situations.

6.1 STPA: Define the purpose of analysis

The STPA analysis aims to prevent future losses in the system comprised of the Fuchs EAF, including its roof, the electrode positioning system, and the furnace cooling system. STPA employs a top-down engineering approach starting with the losses that are unacceptable to stakeholders. In this case, the losses are the same as stated in CAST:

L-1: Loss of life or injury to people

L-2: Loss of or damage to equipment

L-3: Loss of customer satisfaction

The hazards and safety constraints associated with the incident are:

H-1: Furnace integrity is lost [L-1, L-2, L-3]

The safety control structure must ensure:

- **SC-1:** Furnace integrity must be guaranteed under worst-case conditions.
- **SC-2:** The furnace needs to be monitored to alert abnormal operations and take measures to prevent the loss of integrity.

H-2: Furnace cooling is inadequate [L1, L2, L-3]

The safety control structure must ensure:

- **SC-3:** Enforce the control of the cooling system in case the process is out of range, or damage is detected in the shortest time possible.

H-3: Furnace elements collapse or are damaged during operations [L2, L-3]

The safety control structure must ensure:

- **SC-4:** Enforce protections to avoid damages related to contact between moving elements or falling objects.

H-4: Furnace propels dangerous particles to its surroundings [L1, L2]

The safety control structure must ensure:

- **SC-5:** Workers and equipment close to the furnace must be protected from potential impact.
- **SC-6:** The evacuation alarms must be available all times and used when an impact danger exists.

6.2 Model Control Structure

Once the unacceptable losses and the related hazards have been identified, STPA defines the safety control structure of the system.

STPA aims to understand how hazards could occur in the future, so the causes can be eliminated or mitigated during the design phase or before the occurrence of events. In this chapter, the STPA analysis focuses on the dynamics at the operational level of the system that could lead to unacceptable losses. The following figure demonstrates the high-level safety control structure of the system for furnace operations.

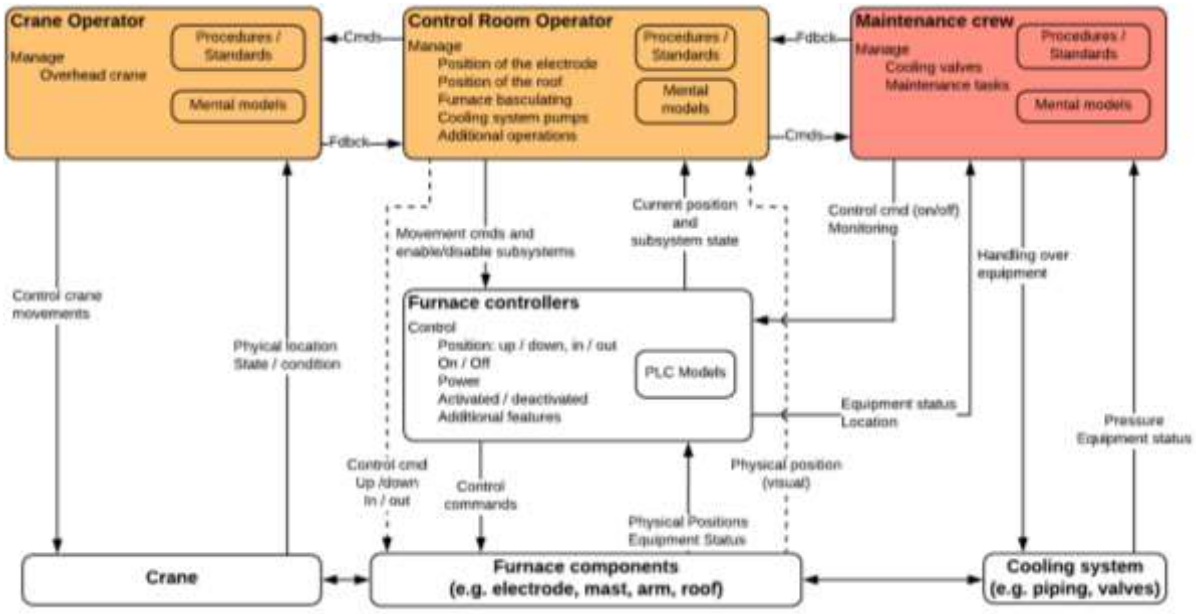


Figure 37: High-Level Safety control structure at operational level

Notice how the control operator acts as a central point in coordinating the activities of other system elements like the crane operator and the maintenance crew. Additionally, the control room operator interacts with several systems through the HMIs to operate the elements of the furnace according to the organization's procedures and his/her individual mental models. Similarly, the maintenance crew interacts with the furnace systems controllers, providing supervision and maintenance to them while receiving commands and feedback from the control room operator about their performance. On the other hand, the crane operator receives the commands from the control room operator to perform the tasks required to perform the steel making process (e.g. hook the electrode to replace it, move a scrap basket to charge the furnace).

The following figure shows, in detail, the interactions between elements considering the control room operator as the fulcrum of the operations:

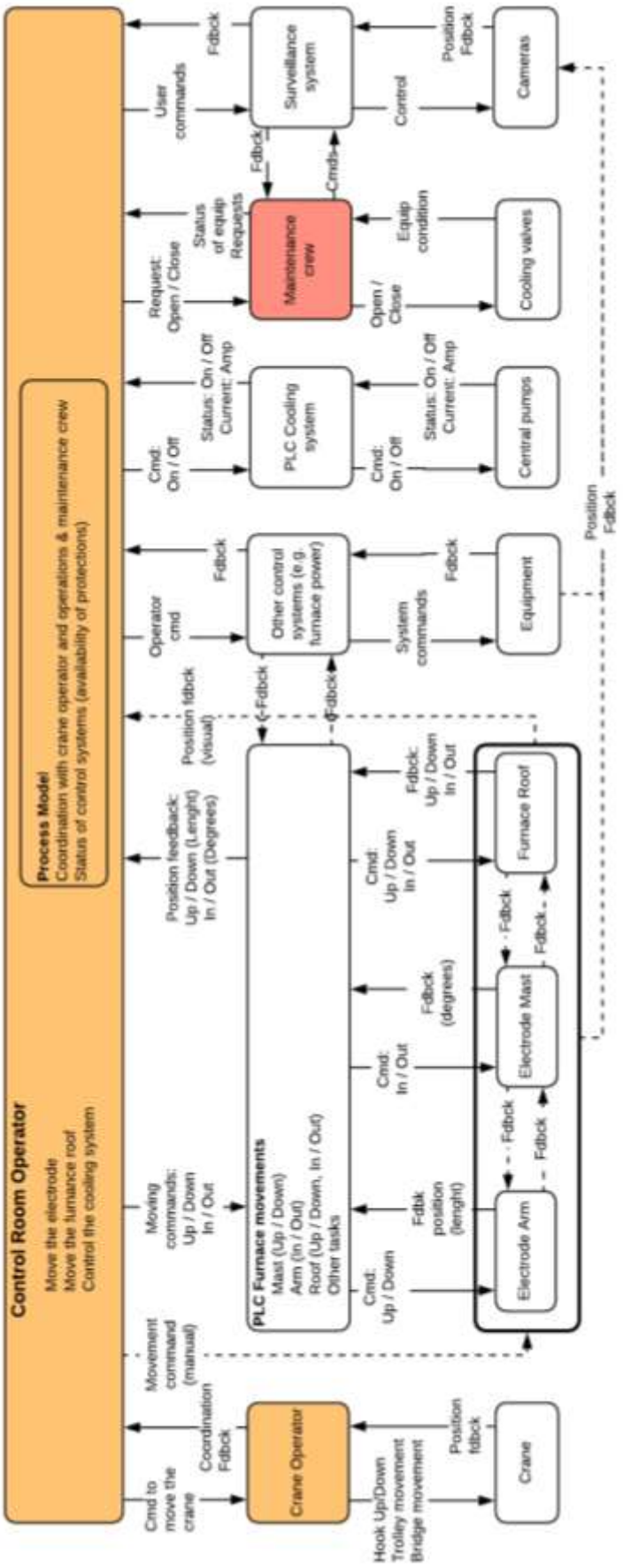


Figure 38: Detailed safety control structure for systems controlled by the control room operator

The detail model includes the specific components of the furnace subject of this analysis (e.g. the mast, arm and furnace roof), as well other systems that were part of the dynamics of the incident. It is interesting to notice that the cooling valves cannot be monitored or operated by the control room operator; the maintenance crew is responsible to handle the valves when necessary. The surveillance system is shown in the figure, and it plays an important role in determining the location of a potential water leak. In the incident that occurred, it also served as an essential tool to document the event for further analysis.

For the purpose of this thesis, the STPA analysis will be restricted only to the interactions between the control room operator, the controllers and the components of the furnace; focusing on the causes that particularly could lead to the Hazard H-3 (Furnace elements collapsed or are damaged during operations).

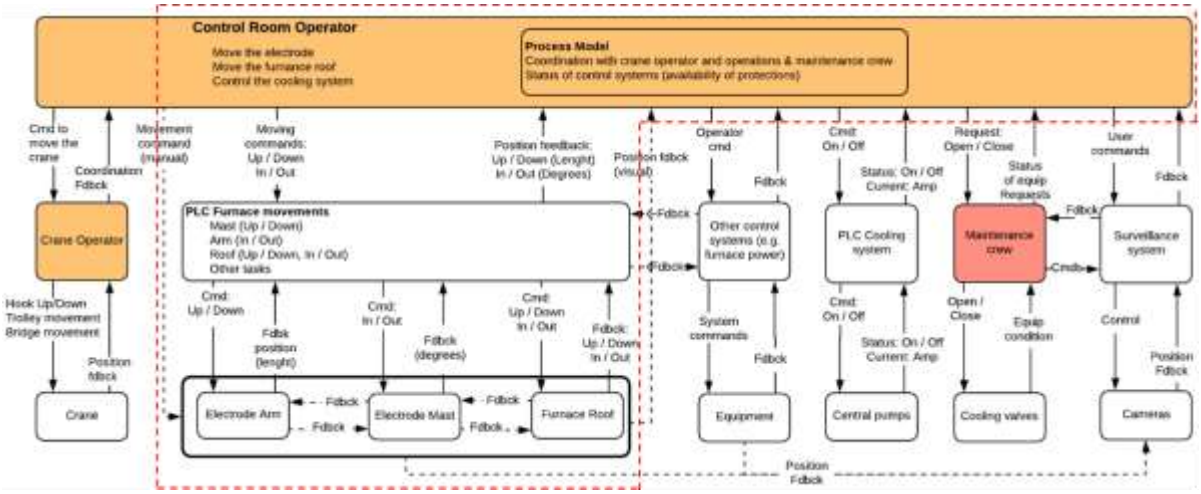


Figure 39: Subsystem considered for the STPA analysis

The following figure illustrates the elements subject to study and the possible movements and positions they could have.

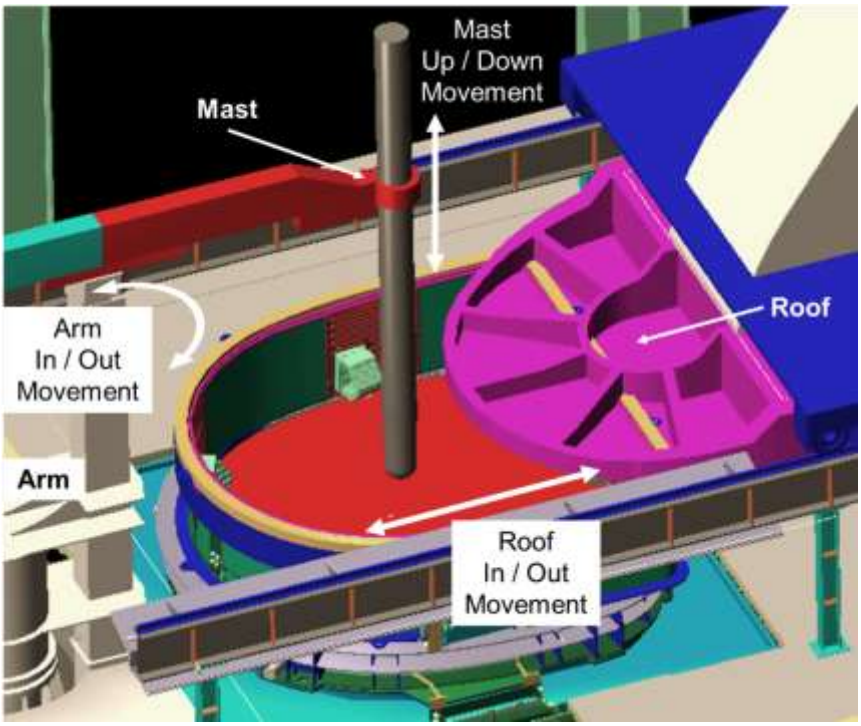


Figure 40: Fuchs furnace components and its movements

6.3 Identifying Unsafe Control Actions

Once the safety control structure is modeled, the next step is to identify the unsafe control actions that could lead to a hazard.

Since this chapter is focused on to the interactions between the control room operator, the controllers, and specific components of the furnace, the UCAs presented here only represent a sample of a full analysis. In Appendix 5, a more complete list of unsafe control actions is presented.

Table 28: Selected UCAs to perform the STPA Analysis

Component	Control Action	Not providing causes hazards	Providing causes hazards	Wrong timing / Order causes hazard	Stopped too soon or applied too long
Mast Electrode position (up / down)	Operator commands to raise the electrode	UCA-1: Operator does not provide mast raise cmd when electrode is inserted and there is an emergency requiring immediate shutdown	UCA-2: Operator provides mast raise cmd when furnace roof is not parked in the fully closed position	UCA:3 Operator provides mast raise cmd too soon when the electrode is inserted before roof furnace has stopped moving	UCA-5: Operator continues providing mast raise cmd too long after electrode is already at its top position when furnace is in operation
Roof position (open / close)	Operator commands to open the roof	UCA-11: Operator does not provide roof open cmd when there is an emergency requiring immediate shutdown	UCA-12: Operator provides open roof cmd when electrode is inserted	UCA-13: Operator provides roof open cmd too early before the electrode has cleared the roof	UCA-15: Operator continues providing roof open cmd too long after the roof is already at its parked position
Mast Electrode position (up / down)	PLC commands to raise the mast	UCA-19: PLC does not provide mast raise cmd when operator commands electrode raise and the electrode is inside the furnace	UCA-20: PLC provides mast raise cmd when mast is already at maximum position	UCA-22: PLC responds too late to raise the mast when an emergency condition requires immediate shutdown	UCA-23: PLC stops providing the mast raise cmd too soon before the mast reaches its top position

Notice that UCA-12 and UCA-19 are exactly what happened during this incident. The other UCAs did not occur in this particular incident, but are just as important to consider in terms of preventing future accidents. Also notice that all of these UCAs can be derived easily and systematically and do not require previous knowledge of the incident.

6.3.1 Identifying Accident Scenarios

After having defined the UCAs and the controller constraints, the next step is to define the scenarios describing the causal factors that can lead to the unsafe control actions. For this purpose, the proposed scenarios should answer these questions:

- Why would the unsafe control action occur?

- Why would control actions be improperly executed or not executed, leading to a hazard?

The following figure shows a refined safety control structure for analyzing the UCAs in the previous section. It includes additional detail related to the interactions between the control room operator, controller, actuators, sensors, and the equipment related to these control actions and decisions.

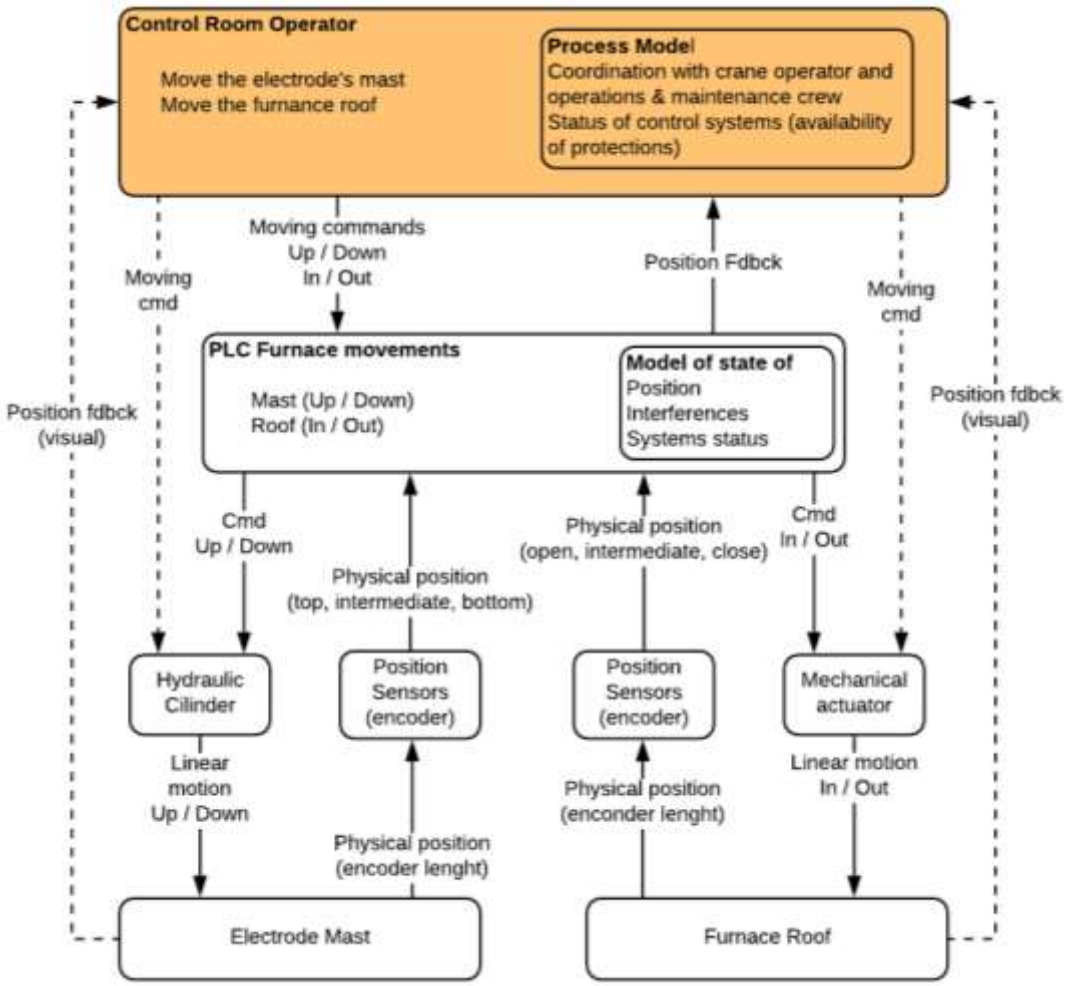


Figure 41: Detail of control structure for the selected UCAs

In general, the scenarios leading to UCAs may involve:

- Failures related to the physical controller
- Inadequate control algorithm
- Unsafe control inputs
- Inadequate process models

Considering these factors, the following scenarios demonstrate the types of problems that STPA identifies.

UCA-1: *Operator does not provide mast raise command when electrode is inserted and there is an emergency requiring immediate shutdown.*

- **PM-1:** The operator does not provide these commands because he/she believes there is no emergency.
  This could be due to:
  - There is a water leak that is detected by personnel on the ground, but it is not communicated to the operator.
  - There is a water leak that is detected by personnel, but it is incorrectly assessed as being insignificant and tolerable.
  - There is a water leak, but it is not detected by personnel on the ground.
  - The operator has not received adequate training to determine that the mast must be raised in an emergency situation.
- **PM-2:** The operator does not provide these commands because he/she believes there is an emergency, but shutdown is not needed.
  This could be due to:
  - There is a water leak that is detected by personnel, but its magnitude is considered as tolerable.
  - There is a water leak that is detected by personnel, but the leak is evaluated as non-critical to shut down since the water is not getting inside the furnace.
- **PM-3:** The operator does not provide these commands because he/she believes the electrode is already sufficiently removed.
  This could be due to:
  - No feedback about the measured electrode height position is provided to the operator (visual feedback only, which is inadequate when furnace is running).
  - Electrode position feedback on glass (tape indication) is removed.
  - Electrode position feedback on glass (tape indication) is changed or the environment changes without updating the tape position.

UCA-2: *Operator provides mast raise command when furnace roof is not parked in the fully closed position.*

- **PM-4:** The operator provides the mast raise command because he/she incorrectly assumes the roof is already in its fully closed position.

This could be due to:

- No feedback is provided to the operator (only visual feedback, which is inadequate when furnace is running).
- Incorrect feedback from furnace roof sensors
  - Could be due to a physical failure of the instrument.
  - Could be due to false readings of the instrument.

- **PM-5:** The operator provides the mast raise command because he/she believes there is enough room to move the electrode.

  This could be due to:
  - The operator has a non-standardized visual reference of the furnace roof to determine when it is safe to move the electrode.
  - The operator has performed this activity in the past without negative outcomes (outcome bias).
  - The operator receives inaccurate feedback from personnel on the floor.

UCA:3 *Operator provides mast raise command too soon when the electrode is inserted before roof furnace has stopped moving.*

- **PM-6:** The operator provides this command because he/she incorrectly assumes there is no risk to perform both activities simultaneously.

  This could be due to:
  - The operator has performed this activity in the past without negative outcomes (outcome bias).
  - Operational procedures do not restrict both movements in parallel.
  - System control allows performing both tasks in parallel.
  - The operator does not have precise position feedback of the mast and roof to determine the adequate moment to safety perform these tasks.
- **PM-7:** The operator provides this command because he/she believes it is possible to perform the tasks more efficiently.

  This could be due to:
  - The operator has stronger incentives or directives to increase productivity than operate safely.

UCA-5: *Operator continues providing mast raise command too long after electrode is already at its top position.*

- **PM-8:** The operator provides this command because he believes the electrode has not reached its top position.

  This could be due to:
  - The operator does not have precise indication of position of the electrode.
  - The operator does not have clear indication when to stop providing the command.
- **PM-9:** The operator continues providing this command because he/she wants to ensure the electrode has reached its top position.

  This could be due to:
  - The operator does not assess or is not aware of the potential damage to equipment related to this task.
  - The operator has experienced in the past issues to reach the electrode's top position.

UCA-11: *Operator does not provide roof open command when there is an emergency requiring immediate shutdown.*

- **PM-10:** The operator does not provide this command because he/she believes the situation does not really represent an emergency.

  This could be due to:
  - The operator has performed this activity in the past without negative outcomes (outcome bias)
  - Incorrect indication from sensors that parameters are within tolerance and there is no emergency
    - Could be due to physical degradation and/or failure of the instruments.
    - Could be due to missing sensors (e.g. no sensors to detect the position).
    - Could be due to existing sensors that are working but inadequate to detect emergency.
    - Incorrect sensors calibration.
    - False detections due to an inadequate selection of sensors.
    - Inadequate location of the sensor causing false detections.
    - Inadequate installation of the sensor causing false detections.
    - Alerts are inadequately defined.
    - Alerts thresholds are incorrectly set.
    - Alerts are inadequately notified to operator.
  - The operator has not received adequate training to determine emergency situations.
- **PM-11:** The operator does not provide these commands because he/she believes it is not required according to the emergency.

  This could be due to:

- Emergency procedures are not adequately defined and documented.
- The operator has not received adequate training to determine emergency situations.

UCA-12: *Operator provides open roof command when electrode is inserted in the furnace.*

- **PM-12:** The operator provides this command because he/she believes the electrode is not inserted.

  This could be due to:
  - The operator does not have feedback about the electrode's position
  - The feedback of the electrode's position is incorrect
  - The operator does not have a reference to contrast and validate the position of the electrode
- **PM-13:** The operator opens the roof because he/she believes the electrode has cleared the furnace roof.

  This could be due to:
  - The operator receives an incorrect feedback due to a failure of the position sensor of the electrode's mast.
  - The operator does not have a precise indication of the position of the lower end of the electrode.
  - The operator does not have a reliable mechanism to verify the position of the electrode and whether it is clear of the roof.
  - The position sensors of the electrode's mast provide incorrect indication
    - Could be due to physical degradation and/or failure of the instruments
    - Incorrect sensors calibration
    - Inadequate algorithm to calculate the position of the electrode

UCA-13: *Operator provides roof open command too early before the electrode has cleared the roof.*

- **PM-14:** The operator provides this command because he/she assumes the electrode has cleared the roof.

  This could be due to:
  - The operator receives incorrect feedback due to a failure of the position sensor of the electrode's mast.
  - The operator does not have a precise indication of the position of the lower end of the electrode.

  - The operator does not have a reliable mechanism to verify the position of the electrode and whether it is clear of the roof.
  - The position sensors of the electrode's mast provide incorrect indication
    - Could be due to physical degradation and/or failure of the instruments
    - Incorrect sensors calibration
    - Inadequate algorithm to calculate the position of the electrode
- **PM-15:** The operator provides this command because he/she assumes both tasks can be performed simultaneously without risk.

  This could be due to:
  - The operator has performed this activity in the past without negative outcomes (outcome bias).
  - Operational procedures do not restrict both movements in parallel.
  - System control allows performing both tasks in parallel.
  - The operator does not have precise position feedback of the mast and roof to determine the adequate moment to safely perform these tasks.

UCA-15: *Operator continues providing roof open command too long after the roof is already at its parked position.*

- **PM-16:** The operator provides this command because he/she assumes the roof has not reached its parked position.

  This could be due to:
  - The operator does not have precise indication of position of the roof.
  - The operator does not have clear indication when to stop providing the command.
- **PM-17:** The operator continues providing this command because he wants to ensure the roof has reached its parked position.

  This could be due to:
  - The operator does not assess the potential damage to equipment related to this task.

UCA-19: *PLC does not provide mast raise command when operator commands electrode raise, and the electrode is inside the furnace.*

- **PM-18:** The PLC does not provide the mast raise command because it does not detect the operator command.

  This could be due to:
  - Failure in the PLC due to degradation or over saturation
  - Failure in the HMI to detect the button command (button failure)

- The HMI button is not properly linked to PLC (wired issue)
- The HMI button is not well configured (algorithm issue)

- **PM-19:** The PLC does not provide the mast raise command because there is a conflict in the algorithm.

  This could be due to:
  - Design flaw in the algorithm of the movement sequences.
- **PM-20:** The PLC does not provide the mast raise command because it detects there is a false obstruction to move upward the electrode.

  This situation could be due to:
  - Incorrect indication from position sensors of furnace components
    - Could be due to physical degradation and/or failure of the instruments
    - Incorrect sensors calibration
    - False detections due to an inadequate selection of sensors
    - Inadequate location of the sensor causing false readings
    - Inadequate installation of the sensor causing false readings
    - Control protections are inadequately configured

UCA-20: *PLC provides mast raise command when mast is at its maximum position.*

- **PM-21:** The PLC provides this command because it does not believe the mast is at its maximum position.

  This could be due to:
  - The position sensor of the mast does not provide feedback.
  - The position sensor of the mast provides incorrect feedback.
  - The system does not have a robust design to determine when is the mast at its top position.

UCA-22: *PLC responds too late to raise the mast when an emergency condition requires immediate shutdown.*

- **PM-22:** The PLC does not perform on time the mast raise command because it does not believe there is an emergency condition or does not believe the operator has commanded mast raise.

  This could be due to:
  - Signals are not adequately transmitted
  - Intense network traffic, saturated switches
  - Inadequate design of communication protocol

- Drivers are outdated

UCA-23: *PLC stops providing the mast raise cmd too soon before the mast reaches its top position.*

- **PM-23:** The PLC stops commanding the upward movement of the mast before reaching its top position because it believes the mast is already at its top position.
  This could be due to:
  - The slow speed ramp is due to a by-pass in the vertical hydraulic cylinder
  - The slow speed ramp is due to an excessive friction in the cylinder caused by physical wear or damage
  - The control speed ramp is inadequately defined in the PLC
  - The system does not have a mechanism to validate the position of the mast

The list of scenarios described before represents a sample of the plausible scenarios that may lead to accidents if they are not properly addressed. However, the list is not exhaustive as is not the purpose of this thesis to perform a complete STPA hazard analysis of the full system. The purpose of this chapter is to evaluate whether STPA would be effective at anticipating and potentially preventing this incident before it occurred.

6.3.2 Safety Requirements

After having defined the UCAs and the possible scenarios of failure, the safety requirements (R) that could be generated are presented hereunder.

- **R1:** Operator must provide mast raise command when electrode is inserted and there is an emergency requiring immediate shutdown.
- **R2:** Operator must not provide mast raise command when furnace roof is not parked in the fully closed position.
- **R3:** Operator must not provide mast raise command too soon when the electrode is inserted before roof furnace has stopped moving.
- **R4:** Operator continues must not provide mast raise command too long after electrode is already at its top position when furnace is in operation.
- **R5:** Operator must provide roof open command when there is an emergency requiring immediate shutdown.
- **R6:** Operator must not provide open roof command when electrode is inserted.

- **R7:** Operator must not provide roof open command too early before the electrode has cleared the roof.
- **R8:** Operator must not continue to provide roof open command too long after the roof is already at its parked position.
- **R9:** PLC must provide mast raise command when operator commands electrode raise and the electrode is inside the furnace.
- **R10:** PLC must not provide mast raise command when mast is already at maximum position.
- **R11:** PLC must not respond too late to raise the mast when an emergency condition requires immediate shutdown.
- **R12:** PLC must not stop providing the mast raise command too soon before the mast reaches its top position.
- **R13:** Create an effective system to monitor and control leaks. The system should be integrated by passive and actives controls.
  - Passive system: Install process cameras to facilitate the detection of water leaks in the furnace.
  - Active system:
    - Monitor the cooling system parameters (e.g. pressure, temperature, flow) to detect when a leak occurred. The system should be in closed loop with the furnace controls to shut it down if necessary.
    - Install automatic cooling valves remotely operated to improve reaction time in case of an emergency.
    - Design an adequate set of alerts to inform the operators when a leak is detected.
- **R14:** Create a reliable and robust system to monitor and control effectively the position of the moveable elements of the furnace (e.g. mast, arm, roof, furnace). The system must be enforced with control protections to restrict component movements when there is a possibility of collision.
- **R15:** Increase reliability of processes by making them less dependent of coordination between workers. Identify what sequences could be performing automatically.
- **R16:** Perform safety assessments of the current control systems to identify and mitigate risks.
- **R17:** The organization shall study in detail the process alerts required and how to communicate them effectively. The alerts must be easy to understand and follow.
- **R18:** The system control shall be designed under a fail-safe perspective to prevent losses.

- **R19:** Enhance the management of change process to adequately documented changes in conditions, parameters and designs.
- **R20:** The organization shall perform meaningful hazard assessments during the design phase of projects to identify possible flaws that could lead to accidents.
- **R21:** The organization shall have an effective and comprehensive maintenance program. Critical equipment for safety must be prioritize (e.g. sensors, actuators).
- **R22:** The organization shall have a program to replace obsolete equipment, focusing on critical equipment for safety.
- **R23:** The organization shall have a safety review pre-start up to ensure all critical components are working properly.
- **R24:** Define and ensure the adequate competences and skills required by the workforce. Focus on critical positions.
- **R25:** Training programs should have a strong safety awareness content to sensitize the workers about the importance of being prudent while working, in addition to the avoidance of overconfidence.
- **R26:** Review operational procedures focusing on critical activities to ensure their completeness regarding safety.
- **R27:** Enhance communication feedback process. The safety issues reported shall be evaluated, prioritized accordingly, and shall have an effective system to follow up.
- **R28:** The organization shall have a systemic approach to analyze its process safety management across the company.
- **R29:** Walk the talk about safety. The organization shall demonstrate coherence and consistency in its safety message.

6.4 Discussion of STPA Process and Results

The sample of STPA results above, focused on mast and furnace roof operations, found twenty-nine recommendations to mitigate the possibility of safety events. The set of recommendations can be categorized based on the effectiveness in controlling hazards according using the safety engineering hierarchy of control.

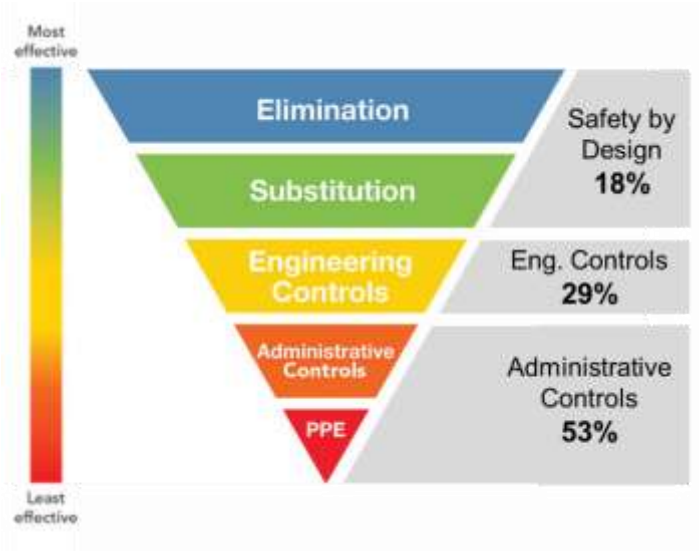


Figure 42: Distribution of recommendations according to the safety hierarchy of control. Modified from [28]

Notice how even from a relatively small number of scenarios above, the analysis uncovered a broad set of factors that designers and management must consider while designing or reviewing the process. Further scenarios and recommendations can be identified by expanding the scope to consider the additional UCAs in Appendix 5. In simple terms, STPA was found to provide a much more complete overview of what could go wrong through an intuitive framework.

Having an easy-to-use systematic framework to analyze safety events is appreciated in the industry. When it comes to understanding the behavior of complex systems and identifying the broad range of causal factors that lead to losses, it is important to have a structured step-by-step approach. Otherwise, the analyst could get lost in the whole range of possibilities.

In this analysis, STPA was found to provide a straightforward way to anticipate the UCAs related to the movements of the mast and the furnace roof that occurred in the incident from the previous chapter.

6.5 Could the STPA approach work if someone does not know the event and is not an expert in STPA?

This section seeks to understand how difficult it could be for people not familiar with the method, and without expertise in the field where the safety event occurred, to perform a hazard assessment using STPA.

For this purpose, four interviews were conducted with company workers from different technical backgrounds, with no formal training in STPA, and with no expertise in steel making. All interviews were conducted separately, and the participants did not exchange information previously, during, or after the discussions.

During the interviews, the participants were first provided with a brief introduction to the method to later perform an STPA trial. Once the foundations of the model have been provided, hence, the description of the operation was explained, as well as basic concepts of steel making focusing on the movements performed by the furnace components. Each individual session last for one and a half hours.

Having explained the basis of STPA and the dynamics of the operation including control actions and the basic control structure, the participants were asked to identify the UCAs for the defined subsystem that includes the electrode´s mast and the furnace roof. The control actions subject to analysis were: 1) operator provides command to raise the electrode; 2) Operator provides command to open the roof.

The interviewed persons identified, in total, eight final distinct UCAs and many of the individual answers overlapped with others. The identified UCAs are shown in the next table:

Table 29: UCAs identified by participants in STPA tests

Control Action	Not providing causes hazards	Providing causes hazards	Wrong timing / Order causes hazard	Stopped too soon or applied too long
Operator provides command to raise the electrode	UCA-1: Operator does not provide the raise mast cmd when there is an emergency	UCA-2: Operator provides raise mast cmd when the roof furnace is not parked	Not considered	Not considered
		UCA-3: Operator provides raise mast cmd when the roof furnace is not centered in its operation position		
		UCA-4: Operator provides raise mast cmd during the meltdown process		
Operator provides command to open the roof	UCA-5: Operator does not open the roof when there is a severe water leak	UCA-7: Operator provides open roof cmd when the electrode is not in its safe position (top position) (x3)	Not considered	Not considered
	UCA-6: Operator does not provide open roof cmd when the steelmaking cycle is over	UCA-8: Operator provides open roof cmd when there is accumulated water inside of the furnace		

The participants pointed out how easy it was to follow the process and identify the unsafe control actions. They remarked that by considering those situations, the model forced you to think what could go wrong under different views, including some of them that were not naturally detected. This result is particularly important as the participant did not have a background in steel making, however, they were able to detect a significant number of conditions that must be prevented to avoid accidents.

Another point the participants noticed was that STPA strongly focused on the interactions between the elements of the system. This result was particularly interesting to them, as this point is not typically addressed by the models used in the industry to analyze safety events. They discovered the importance of studying these interactions at different levels (organizational, human operator, software, and hardware) to determine different gaps that could lead to an accident.

One point that came out during the interviews, was the concern about how to handle and prioritize the unsafe control actions and recommendations. All of the participants agreed that the STPA model is relatively easy to follow and comprehensive; however, for practical

purposes in the daily industry life, they were interested to know if the model suggests a method to manage the outcomes as a guide towards a plan execution. They were interested to know how to organize and prioritize all the valuable outcomes gained from the analysis.

They noticed the importance of having an instructor through the analysis process, primarily when the participants are not familiar with the model, to have a more productive work session. Some participants asked if STPA has support software to facilitate the analysis, like the HAZOP software available on the market. This functionality could be useful to provide as a tool to design the control structure diagrams, to guide the definition of the UCAs, as well for document purposes.

Finally, the participants considered whether the STPA method could be easily replicated for other industry processes as it could provide important results for companies. In their opinion, STPA is a powerful tool suitable to understand complex systems in an intuitive and organized way. They would like to see a practical and complimentary approach to put it into practice (e.g. using a software), and a suggested method to prioritize the outcomes of the analysis (e.g. rank the UCAs by relevance).

Chapter 7: Conclusions

7.1 Conclusions and Recommendations

The steel industry has evolved in recent years incorporating new technologies to make processes more productive and safer at the same time. Particularly, automation has reshaped the way steel is produced and the way the personnel interact with the processes. Not many years ago, steelworkers had to perform several activities under precarious conditions, exposing themselves to high risks. Extraordinary efforts have been made recently to improve these conditions throughout the industry; however, there is still a long way to go regarding safety.

STAMP has proven to be a powerful model for understanding the safety dynamics of complex systems, including those present in the steel industry. Its holistic approach and guided framework allow thinking beyond what is ordinarily evident. This thesis presented a contrast between the outcomes from traditional methods and new “systems-thinking” methods –CAST and STPA—when analyzing a real case from the steel industry. In this case, traditional methods covered only a few of the factors involved, focusing mainly on physical aspects such as equipment failures and trivial human causes such as not following procedures and inadequate coordination between personnel.

However, the contextual circumstances, process models, mental model beliefs, the interactions between system components, and systemic factors were not correctly scrutinized by these models. The desire to simplify the causality and focus only on obvious trivial factors misleads the analysis and obscures the underlying factors that led to the event. Organizations are trying to shoehorn the current industrial reality into limited methods, and finding similar events happening again and again. This does not mean that these old models are completely invalid, but they are incomplete. Analysts need to recognize their limitations and shortcomings, and these gaps need to be addressed.

Safety is a never-ending effort. Rasmussen [29], stated that safety degrades in the absence of conscious effort. Safety needs to embedded in the culture of companies and put at the forefront of their decisions. STAMP aims to help the pursuing of this cultural shift. By analyzing the causality of events with a broader and systemic perspective, organizations can understand the deeper factors and circumstances that are leading to accidents. To be effective, CAST and STPA requires a certain level of maturity and willingness to improve from organizations. These approaches enable a deep introspection into the safety dynamics of the company,

allowing them to uncover and understand the behavior and beliefs of workers, management, and the organization as a whole.

This thesis evaluated the benefits of CAST and STPA when applied to a real system and a real case from the industry. Undoubtedly, the completeness of these analyses is superior to the detail obtained from other models such as RCA. A more detailed analysis would allow organizations to prevent undesirable losses and be proactive about future casualties instead of reactive. These losses also affect the sustainability of the business; safety is not only a matter of human lives, but it can also have a significant impact on the economic performance of companies. Organizations need to formulate strategies to incorporate safety not only as a requirement, but as an inherent value and a way to do business.

STPA proved to be an intuitive and robust tool to determine what could go wrong during operations. This thesis analyzed only a sample of UCAs and scenarios related to a physical system from the Fuchs EAF. Although the analysis was constrained, the outcomes demonstrated that the actions and behaviors that led to the incident would have been anticipated by using this approach, and more effective controls potentially could have been put in place before it occurred. Using these results, companies can better design the process and its control, design the equipment required, the necessary procedures, and even define the required competences and skills from personnel. STPA, throughout its framework, guides the analyst to study these and other factors to define the appropriate constraints and ensure the overall safety control structure enforces them.

CAST and STPA can improve the way safety is approached. Both approaches were found to be suitable for the steel industry and provide a new perspective of accident causality that broadens the traditional views. This thesis could be used to introduce these new concepts to the steel industry by showing their applicability and benefits for a real cast study.

However, traditional models have been used by the steel industry for decades and they are well established with many organizations familiar with them. Of course, a change in the safety approach will not happen overnight. Considering this, the following section provides suggestions to implement STAMP in large organizations that are currently using the traditional accident models.

7.2 Suggested implementation roadmap of STAMP in large organizations

Change can be difficult, particularly in organizations that have been working for a long time with traditional safety models. Therefore, a roadmap to achieve a successful implementation is desirable.

First, organizations need to start identifying and recognizing why they need to change their safety approach, what are the gaps they need to fill, and what they want to achieve through this change. Organizations should recognize that a systemic approach is needed to move forward towards a safer state. Management sponsorship and commitment for improvement will be fundamental in the pursuit of this objective.

Once the organization and its management are engaged and committed to improving safety, it is recommended to identify a sweet spot to initiate the application of STAMP. Companies might focus on a few initiatives like a pilot study to evaluate the approach themselves, build confidence in it, and to gain momentum. An organization could begin with a CAST analysis of incidents or accidents that have had a significant impact (e.g., a high-risk incident or accident). Likewise, STPA can be evaluated for modification projects or new installations. During this process, it is important to note that the purpose of these methods is not to cast blame. More importantly, they aim to understand the underlying causes that are leading or could lead to safety events.

To perform the analyses, it is recommended to form an interdisciplinary group to have different perspectives and knowledge areas based on the control structure. Training in the methods is important to grasp the concepts and to ensure their effective implementation. It is recommended to identify the best candidates for training to allow a critical mass to be created and to ensure the sustainability and growth of this initiative.

Once the initial group has been trained and the analyses have demonstrated value vis-a-vis traditional models, the organization should start to recognize CAST and STPA as part of its internal safety management process. The company can then begin to expand the application of these approaches beyond the initial cases and could start to increase the number of people trained in the model.

The timing of this implementation could depend on the organization. Some companies are more open to changes. For them, it could be easier to grasp the new concepts and deploy it throughout the organization relatively fast (within a few months). For some others, they could find a reluctance to change inside the organization, and probably will require more time to adapt its structure to make systems approaches like CAST and STPA part of their daily life.

Nevertheless, taking the first step is the most important. If this project is taken on by organizations with a genuine commitment to improve and an openness to change if needed, the results from CAST and STPA will be noticed and the companies will move towards a safer and sustainable state.

7.3 Future work

CAST and STPA are extraordinary methods to analyze past and future accident that otherwise could be oversimplified or only superficially examined by organizations. Their comprehensive approach allows analyzing the systems with a rich and broad perspective.

One of the challenges while applying these methods is how to prioritize all the causes and recommendations that come out of the analysis. While all of them are relevant, organizations may not have resources to face them all immediately and simultaneously. So, prioritization is useful to ensure the desired evolution of the system regarding safety. Past work has examined prioritization based on severity, controllability, and importance. Future work could further explore the most effective mechanism for prioritization using these or other factors.

Another source for future work is the integration of data analytics to support the analysis of CAST and STPA. This area represents an exciting field to study. Data analytics could supply hard information to complement the analyses and reinforce the expertise and judgment from the personnel involved in the examination of past or future events.

References

[1] Friedman, T. L. (2017). *Thank you for being late an optimists guide to thriving in the age of accelerations.* Farmington Hills, MI: Thorndike Press, a part of Gale, Cengage Learning.

[2] Safety and health in the steel industry. Position Paper. (2018). Retrieved March 1, 2019, from https://www.worldsteel.org

[3] Leveson, N. (2012). *Engineering a safer world: systems thinking applied to safety.* Cambridge, Mass.: MIT Press.

[4] The white book of steel. (2012). Retrieved March 1, 2019, from https://www.worldsteel.org/

[5] Steel Facts. (2018). Retrieved March 1, 2019, from https://www.worldsteel.org/about-steel/steel-facts.html

[6] Interactive Steel Manufacturing Process. (2015). Retrieved March 3, 2019, from http://www.aist.org/resources/the-msts-steel-wheel

[7] Heinrich, H. W. (1969). *Industrial accident prevention: A scientific approach.* New York: McGraw-Hill.

[8] Reason, J. (2009). *Human Error*. Cambridge: Cambridge University Press.

[9] U.S Department of Energy. (1992). Root Cause Analysis Guidance Document. Retrieved March 30, 2019, from https://www.env.nm.gov/aqb/documents/DOERootCause AnalysisGuidanceManual.pdf.

[10] File:Root Cause Analysis Tree Diagram.jpg. (2016, November 21). Wikimedia Commons, the free media repository. Retrieved 04:23, June 30, 2019 from https://commons.wikimedia.org/w/index.php?title=File:Root_Cause_Analysis_Tree_Diagram.jpg&oldid=216923442.

[11] Latino, K. C. (2011). *Root cause analysis: Improving performance for bottom line results* (4th ed.). Boca Raton, FL: CRC Press.

[12] Crawley, F., Preston, M., & Tyler, B. (2008). *HAZOP: Guide to best practice for the process and chemical industries*. Rugby: IChemE.

[13] Dunjó, J., et al. (2010). Hazard and operability (HAZOP) analysis. A literature review. *Journal of Hazardous Materials*. 173(1–3): p. 19-32.

[14] Stringfellow, M. (2010). *Accident Analysis and Hazard Analysis for Human and Organizational Factors*. (Doctoral dissertation). MIT. Cambridge.

[15] Leveson, N. & Thomas, J. (2018). *STPA Handbook.* MIT Partnership for Systems Approaches to Safety. Available at:

https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

[16] Seetharaman, S., McLean, A., Guthrie, R. I., & Sridhar, S. (2014). *Treatise on process metallurgy: Industrial Processes* (Vol. 3).

[17] Tupkary, R. H., & Tupkary, V. R. (2018). *Modern steel making handbook.* Retrieved from https://app.knovel.com/hotlink/toc/id:kpMSMH000P/modern-steel-making-handbook/modern-steel-making-handbook.

[18] Hyten, C., & Ludwig, T. D. (2017). Complacency in Process Safety: A Behavior Analysis Toward Prevention Strategies. *Journal of Organizational Behavior Management*, 37(3-4), 240-260. doi:10.1080/01608061.2017.1341860

[19] Fernández-Muñiz, B., Montes-Peón, J. M., & Vázquez-Ordás, C. J. (2017). The role of safety leadership and working conditions in safety performance in process industries. *Journal of Loss Prevention in the Process Industries*, 50, 403-415. doi:10.1016/j.jlp.2017.11.001

[20] Hulin, B., & Tschachtli, R. (2011). Identifying Software Hazards with a Modified CHAZOP. *PESARO 2011: The First International Conference on Performance, Safety and Robustness in Complex Systems and Applications.*

[21] Davey, L. et al. (2016, September 12). How to Put the Right Amount of Pressure on Your Team. Retrieved June 29, 2019, from https://hbr.org/2016/07/how-to-put-the-right-amount-of-pressure-on-your-team

[22] Thomas, J. (2013). *Extending and automating a systems-theoretic hazard analysis for requirements generation and analysis.* (Doctoral dissertation). MIT. Cambridge.

[23] Leveson, N. G. (2001). *Safeware: System safety and computers*. Boston, MA: Addison-Wesley.

[24] Leveson, N. (2012). *Engineering a safer and more secure world.* Unpublished document.

[25] Hazard prevention and control. (2019). Retrieved July 11, 2019, from https://www.osha.gov/shpguidelines/hazard-prevention.html

[26] Rasmussen, Jens. (1997). Risk Management in a Dynamic Society: A Modelling Problem. *Safety Science*. Vol. 27, No. 2/3. pp. 183-213.

[27] Center for Chemical Process Safety/AIChE. (2018). *Bow Ties in Risk Management - A Concept Book for Process Safety.* Center for Chemical Process Safety/AIChE. Retrieved from https://app.knovel.com/hotlink/toc/id:kpBTRMACB3/bow-ties-in-risk-management/bow-ties-in-risk-management

Appendix 1: Interactions in safety control structure. Safety Team & Corporate Management

The tables shown in the Appendices describe in detail the interactions between elements of the safety control structure.

The description in the cells represent the activities and tasks performed by the controllers on the row, while the controllers on the column constitute the stakeholders of those activities and tasks. The cells on gray portray the lack of interaction between elements.

	Safety Engineer	**Safety Management**	**Corporate Management**
Engineering Worker	- Report safety anomalies and warnings (stds deviations, incidents, accidents) - Requests authorization to perform restricted activities (entry to confine spaces, welding)		
Project Manager	- Report safety anomalies and warnings (stds deviations, incidents, accidents) - Requests authorization to perform restricted activities (entry to confine spaces, welding)		
Engineering Management		- Communicate the project plan: scope, budget, schedule, and support needed from safety. - Report safety anomalies and warnings (stds deviations, incidents, accidents)	- Communicate the project plan: scope, budget, schedule, limitations and exclusions. - Request project approval. - Inform on timely maner the performance of the project according to scope, budget and schedule. - Inform the results of the project's risk assessment
Main Control Room Operator	- Report safety anomalies and warnings (stds deviations, incidents, accidents) - Requests authorization to perform restricted activities (entry to confine spaces, welding)		
Operations Crew	- Report safety anomalies and warnings (stds deviations, incidents, accidents) - Requests authorization to perform restricted activities (entry to confine spaces, welding)		
Furnace Crane Operator	- Report safety anomalies and warnings (stds deviations, incidents, accidents) - Requests authorization to perform restricted activities (entry to confine spaces, welding)		
Operations Engineers & Sups	- Report safety anomalies and warnings (stds deviations, incidents, accidents) - Requests authorization to perform restricted activities (entry to confine spaces, welding)		
Operations Management		- Communicate project plan: scope, budget, schedule, and support needed from safety. - Report safety anomalies and warnings (stds deviations, incidents, accidents)	- Communicate the project plan: scope, budget, schedule, limitations and exclusions. - Inform on timely maner the performance of the project according to scope and schedule.
Maintenance Contractors	- Report safety anomalies and warnings (stds deviations, incidents, accidents) - Requests authorization to perform restricted activities (entry to confine spaces, welding)		
Maintenance Technicians	- Report safety anomalies and warnings (stds deviations, incidents, accidents) - Requests authorization to perform restricted activities (entry to confine spaces, welding)		
Maintenance Leaders & Sup	- Report safety anomalies and warnings (stds deviations, incidents, accidents) - Requests authorization to perform restricted activities (entry to confine spaces, welding)		
Maintenance Management		- Communicate project plan: scope, budget, schedule, and support needed from safety. - Report safety anomalies and warnings (stds deviations, incidents, accidents) - Allocate resources accordingly	- Communicate the project plan: scope, budget, schedule, limitations and exclusions. - Inform on timely maner the performance of the project according to scope and schedule.
Safety Engineer		- Provide timely report about the safety performance during the shutdown	
Safety Management	- Allocate resources accordingly - Provide support and guidance to ensure compliance of safety stds		- Inform the hazards and risks of the project, and the measures to mitigate them - Communicate the project performance regarding safety
Corporate Management		- Request good safety performance during the shutdown. - Provide policies and guidelines regarding safety: Safety must be always the top priority.	

Appendix 2: Interactions in safety control structure. Operations Team.

	Main Control Room Operator	Operations Crew	Furnace Crane Operator	Operations Engineers & Supervisors	Operations Management
Engineering Worker	- Requests for support to perform engineering activities (transport and activate equipment, move out people, cleaning) - Communicate if a hazard is detected	- Requests for support to perform engineering activities (transport and activate equipment, move out people, cleaning) - Communicate if a hazard is detected	- Requests for support to perform engineering activities (transport and activate equipment, move out people, cleaning) - Communicate if a hazard is detected		
Project Manager				- Inform and provide design specifications - Provide a hazard analysis of the project - Communicate the project plan: scope, schedule and support needs from the operations team. As well, inform the limitations and exclusions (what is included and what is not)	
Engineering Management					- Inform and provide design specifications for approval - Communicate the project plan: scope, budget, schedule, and support needed from operations. - Inform about the constraints, limitations and exclusions.
Main Control Room Operator		- Request physical inspection and verifications of equipment - Communicate any safety anomalies in during activities	- Request physical inspection and verifications of equipment - Coordinate operations tasks (electrode positioning)	- Report safety anomalies (stds deviations, incidents, accidents) - Approval requests (work authorizations for high risk activities) - Coordinate critical activities (electrode positioning, furnace inspections)	
Operations Crew	- Reporting of physical conditions and positions (interferences) - Communicate any safety anomalies in during activities		- Request support to transport equipment or perform an activity - Communicate any safety anomalies during activities	- Report safety anomalies (stds deviations, incidents, accidents) - Approval requests (work authorizations for high risk activities) - Coordinate critical activities (electrode positioning, furnace inspections)	
Furnace Crane Operator	- Reporting of physical conditions and positions (interferences) - Communicate any safety anomalies in during activities				
Operations Engineers & Sups	- Provide safety stds to workforce and ensure their compliance - Provide guidance and resources to workforce to perform activities according to stds - Verify authorization requests to perform activities safely	- Provide safety stds to workforce and ensure their compliance - Provide guidance and resources to workforce to perform activities according to stds - Verify authorization requests to perform activities safely			- Report safety anomalies (stds deviations, incidents, accidents) - Inform safety warnings and delays in activities - Approval requests (work scheduling)
Operations Management				- Provide safety stds and ensure their compliance (perform audits during the shutdown) - Provide guidance and resources to perform activities according to stds. Ensure previous and during the shutdown the teams have adequate resources.	
Maintenance Contractors					
Maintenance Technicians	- Report equipment condition after inspections - Inform any warning about equipment status - Requests for operations support (turn on/off, move in/out) - Communicate any safety anomalies in during activities				
Maintenance Leaders & Sup				- Inform detected problems in equipment (leaks, damages, out-of-service). - Request operations support (transport equipment, clear areas) - Communicate any safety anomalies during activities	
Maintenance Management					- Coordinate activities to ensure their compliance to safety stds and project plan - Communicate any safety anomalies during activities - Request support to perform maintenance activities (transport and activate equipment, clear areas)
Safety Engineer	- Provide and ensure the compliance of safety stds and regulations (perform audits) - Authorize high risk activities - Supervise activities during the shutdown from safety point of view - Provide support to workforce concerns and doubts about safety	- Provide and ensure the compliance of safety stds and regulations (perform audits) - Authorize high risk activities - Supervise activities during the shutdown from safety point of view - Provide support to workforce concerns and doubts about safety	- Provide and ensure the compliance of safety stds and regulations (perform audits) - Authorize high risk activities - Supervise activities during the shutdown from safety point of view - Provide support to workforce concerns and doubts about safety	- Provide and ensure the compliance of safety stds and regulations (perform audits) - Authorize high risk activities - Supervise activities during the shutdown from safety point of view - Provide support to workforce concerns and doubts about safety	
Safety Management					- Provide and ensure the compliance of safety stds and regulations (perform audits) - Provide support to perform operations hazard analysis - Provide technical support to safety concerns
Corporate Management					- Request compliance of authorized project plan (scope, schedule and budget). No delays are acceptable considering the relevance of the plant to company's operations. - Provide policies and guidelines regarding safety: Safety must be always the top priority.

Appendix 3: Interactions in safety control structure. Maintenance Team.

	Maintenance Contractors	Maintenance Technicians	Maintenance Leaders & Supervisors	Maintenance Managers
Engineering Worker				
Project Manager			- Inform and provide design specifications - Provide a hazard analysis of the project - Communicate the project plan: scope, schedule and support needs from the operations team. As well, inform the limitations and exclusions (what is included and what is not)	
Engineering Management				- Inform and provide design specifications for approval - Communicate the project plan: scope, budget, schedule, and support needed from maintenance. - Inform about the constraints, limitations and exclusions.
Main Control Room Operator		- Report alarms and abnormal conditions (high/low temperature, high/low pressure, high/low level) - Provide support to maintenance activities (turn on/off, report equipment status)		
Operations Crew				
Furnace Crane Operator				
Operations Engineers & Sups			- Inforrm detected problems in equipment (leaks, damages, out-of-service). - Accept & reject equipment according to its condition. - Communicate any safety anomalies during activities - Provide suppor to perform maintenance activities (transport and activate equipment, clear areas)	
Operations Management				- Coordinate activities to ensure their compliance to safety stds and project plan - Communicate any safety anomalies during activities - Provide support to perform maintenance activities (transport and activate equipment, clear areas)
Maintenance Contractors			- Report safety anomalies (stds deviations, incidents, accidents) - Approval requests (work authorizations, work scheduling) - Inquiries about risks and hazards in the area (temperature, electrical, superpositioned activities)	
Maintenance Technicians			- Report safety anomalies (stds deviations, incidents, accidents) - Approval requests (work authorizations for high risk activities) - Coordinate critical activities (activities related with high voltages, access to confine spaces)	
Maintenance Leaders & Sup	- Provide safety stds to workforce and ensure their compliance by audits - Provide guidance and resources to workforce to perform activities according to stds - Verify authorization requests to perform activities safely	- Provide safety stds to workforce and ensure their compliance - Provide guidance and resources to workforce to perform activities according to stds - Verify authorization requests to perform activities safely		- Report safety anomalies (stds deviations, incidents, accidents) - Inform safety warnings and delays in activities - Approval requests (work scheduling)
Maintenance Management			- Provide safety stds and ensure their compliance (perform audits during the shutdown) - Provide guidance and resources to perform activities according to stds. - Ensure previous and during the shutdown the teams have adequate resources.	
Safety Engineer	- Provide and ensure the compliance of safety stds and regulations (perform audits) - Authorize high risk activities - Supervise activities during the shutdown from safety point of view - Provide support to workforce concerns and doubts about safety	- Provide and ensure the compliance of safety stds and regulations (perform audits) - Authorize high risk activities - Supervise activities during the shutdown from safety point of view - Provide support to workforce concerns and doubts about safety	- Provide and ensure the compliance of safety stds and regulations (perform audits) - Authorize high risk activities - Supervise activities during the shutdown from safety point of view - Provide support to workforce concerns and doubts about safety	
Safety Management				- Provide and ensure the compliance of safety stds and regulations (perform audits) - Provide support to perform maintenance hazard analysis - Provide technical support to safety concerns
Corporate Management				- Request compliance of authorized project plan (scope, schedule and budget). No delays are acceptable considering the relevance of the plant to company's operations. - Provide policies and guidelines regarding safety: Safety must be always the top priority.

Appendix 4: Interactions in safety control structure. Engineering Team.

	Engineering Worker	Project Manager	Engineering Management
Engineering Worker		- Report safety anomalies (stds deviations, incidents, accidents) - Approval requests (work authorizations, work scheduling) - Inquiries about risks and hazards in the area (temperature, electrical, superpositioned activities) - Requirements to perform activities safely (safety gear, LOTO)	
Project Manager	- Provide safety stds to workforce and ensure their compliance - Provide guidance and resources to workfore to perform activities according to stds - Verify authorization requests to perform activities safely		- Request approval for project design and implementation plan - Provide on timely manner project updates and safety anomalies - Inform and request approvals for project modifications (technical and budget changes)
Engineering Management		- Provide safety stds to project managers and ensure their compliance - Provide guidance and resources to projects to ensure their performance according to stds	
Plant Operators (crane, control room, operations crew)	- Communicate if the project (new equipment and systems) fulfill user requirements - Provide support to the project to ensure its completion on time and according to stds (move and enable equipment) - Communicate any safety anomalies in project activities		
Operations Engineers & Sups		- Communicate if the project (new equipment and systems) fulfill user requirements - Provide support to the project to ensure its completion on time and according to stds (move and enable equipment) - Communicate any safety anomalies in project activities	
Operations Management			- Inform detailed requirements and needs for projects - Active participation during the design phase - Provide timely feedback to project during design and execution phase - Provide support during execution phase (assign resources to support engineering activities)
Maintenance Technicians & Contractors	- Communicate if the project (new equipment and systems) fulfill requirements - Provide support to the project to ensure its completion on time and according to stds - Communicate any safety anomalies in project activities		
Maintenance Leaders & Sup		- Communicate if the project (new equipment and systems) fulfill requirements - Provide support to the project to ensure its completion on time and according to stds - Communicate any safety anomalies in project activities	
Maintenance Management			- Inform detailed requirements and needs for projects - Active participation during the design phase - Provide timely feedback to project during design and execution phase - Provide support during execution phase
Safety Engineer	- Provide and ensure the compliance of safety stds and regulations (perform audits) - Authorize high risk activities - Supervise activities during the shutdown from safety point of view - Provide support to workforce concerns and doubts about safety	- Provide and ensure the compliance of safety stds and regulations (perform audits) - Provide support to perform project hazard analysis - Authorize high risk activities - Supervise activities during the shutdown from safety point of view	
Safety Management			- Provide and ensure the compliance of safety stds and regulations (perform audits) - Provide support to perform project hazard analysis - Provide technical support to safety concerns
Corporate Management			- Request compliance of authorized project plan (scope, schedule and budget). No delays are acceptable considering the relevance of the plant to company's operations. - Provide policies and guidelines regarding safety: Safety must be always the top priority.

Appendix 5: STPA Unsafe Control Actions

Operator controls the electrode's position

Control Action	Not providing causes hazards	Providing causes hazards	Wrong timing / Order causes hazard	Stopped too soon or applied too long
Operator provides command to raise the electrode	UCA-1: Operator does not provide mast raise cmd when eletrode is inserted and there is an emergency requiring immediate shutdown	UCA-2: Operator provides mast raise cmd when furnace roof is not parked in the fully closed position	UCA:3 Operator provides mast raise cmd too soon when the electrode is inserted before roof furnace has stopped moving	UCA-5: Operator continues providing mast raise cmd too long after electrode is already at its top position when furnace is in operation
			UCA-4: Operator provides mast raise cmd too late after emergency condition requires immediate shutdown	UCA-6: Operator stops providing mast raise cmd too soon before electrode has cleared the roof
Operator provides command to lower the electrode	Not hazardous	UCA-7: Operator provides mast lower cmd when roof furnace is not parked in the fully closed position	UCA-9: Operator provides mast lower cmd too early before roof furnace has stopped moving	UCA-10: Operator continues providing mast lower cmd too long after electrode is already at its lower position
		UCA-8: Operator provides mast lower cmd when the electrode is hooked to the overhead crane		

Operator controls the roof's position

Control Action	Not providing causes hazards	Providing causes hazards	Wrong timing / Order causes hazard	Stopped too soon or applied too long
Operator provides command to open the roof	UCA-11: Operator does not provide roof open cmd when there is an emergency requiring immediate shutdown	UCA-12: Operator provides open roof cmd when electrode is inserted	UCA-13: Operator provides roof open cmd too early before the electrode has cleared the roof	UCA-15: Operator continues providing roof open cmd too long after the roof is already at its parked position
			UCA-14: Operator provides roof open cmd too late after emergency condition requires	

			immediate shutdown	
Operator provides command to close the roof	Not hazardous	UCA-16: Operator provides close roof cmd when electrode is inserted	Not applicable	UCA-18: Operator continues providing roof close cmd too long after the roof is already at its operation position
		UCA-17: Operator provides close roof cmd when water is getting inside of the furnace		

PLC controlling the electrode's position

Control Action	Not providing causes hazards	Providing causes hazards	Wrong timing / Order causes hazard	Stopped too soon or applied too long
PLC provides command to raise the mast	UCA-19: PLC does not provide mast raise cmd when operator commands electrode raise and the electrode is inside the furnace	UCA-20: PLC provides mast raise cmd when mast is already at maximum position	UCA-22: PLC responds too late to raise the mast when an emergency condition requires immediate shutdown	UCA-23: PLC stopped the mast raise cmd too soon before the mast reached its top position
		UCA-21: PLC provides mast raise cmd when the furnace roof is not parked		
PLC provides command to lower the mast	Not hazardous	UCA-24: PLC provides mast lower cmd when furnace roof is not parked in the fully closed position	Not applicable	Not applicable
		UCA-25: PLC provides mast lower cmd when electrode is already at its lower position inside the furnace		

PLC controlling the roof's position

Control Action	Not providing causes hazards	Providing causes hazards	Wrong timing / Order causes hazard	Stopped too soon or applied too long
PLC provides command to open the roof	UCA-26: PLC does not prove open roof cmd when the operator commands roof open during an emergency situation	UCA-28: PLC provides open roof cmd when the electrode has not cleared the roof	UCA-31: PLC responds too late to open the roof when an emergency condition requires immediate shutdown	Not applicable
		UCA-29: PLC provides open roof cmd when the electrode is inserted		
		UCA-30: PLC provides roof open cmd when the roof is fully open		
PLC provides command to close the roof	Not hazardous	UCA-32: PLC provides close roof cmd when the electrode has not cleared the roof	Not applicable	Not applicable
		UCA-33: PLC provides roof close cmd when the electrode is inserted		
		UCA-34: PLC provides roof close cmd when the roof is fully close		