ISSN 1831-9424

Organisation of study and a workshop on

Learning from cross-cutting cooperation with other industries to improve and maintain nuclear safety in the EU

Summary Report

ENCO FR-(12)-70
Mai 2013

Specific Contract No. ENER/ 2011/NUCL/SI2.599383

EUR 25979 EN

Energy

Organisation of study
and a workshop on

Learning from cross-cutting cooperation with other industries to improve and maintain nuclear safety in the EU

Summary Report

ENCO FR-(12)-70
Mai 2013

Specific Contract No. ENER/ 2011/NUCL/SI2.599383

enco

DOCUMENT REVIEW
AND APPROVAL COVER SHEET

PROJECT Nr.:	Framework Service Contract for Technical Assistance TREN/R1/350-2008 Lot 3 Specific Contract No. ENER/ 2011/NUCL/SI2.599383
PROJECT TITLE:	ORGANISATION OF STUDY AND A WORKSHOP ON "LEARNING FROM CROSS CUTTING COOPERATION WITH OTHER INDUSTRIES TO IMPROVE AND MAINTAIN NUCLEAR SAFETY IN THE EU"
PERFORMED BY:	ENCONET
TASK:	Task #12 Summary Report
PREPARED FOR:	EC, DG for ENERGY, ENER D2

DATE released	REVISION	PREPARED/ REVISED by:	REVIEWED by:	APPROVED by:
19.12.2012	0	I.Popa Date: 01.12.2012	E.Hollnagel Date: 17.12.2012	B.Tomic Date: 19.12.2012

Table of Contents

1 INTRODUCTION

1.1 Background

The population's increased sensitivity towards safety is affecting every industry that has potential for affecting the environment and humans, that being the traffic or any kind of manufacturing/production. The nuclear industry together with the aviation, both of which experienced high visibility (and in aviation, consequence) catastrophic events are under the highest scrutiny. Due to the fact that their accidents are less visible, the maritime as well as the chemical industries, while having serious safety concerns of their own, are somehow less scrutinized. Scores of other industries have the safety thinking incorporated in their activities including e.g. medical and pharmaceutical industries.

While all of those industries and in particular their safety concepts have been developing separately, the safety practitioners recognized that the time has come when everyone needs to look over the fence and see whether some safer thinking and solutions could be successfully brought across the divide.

Likely the first systematic look across the divide was undertaken during the pioneering workshop that was organized by the EC TREN H2 (with ENCO being the consultant implementing the activities) in 2007 discussing "Regulations and enforcement in Aviation, Maritime and Nuclear (A, M, N) industries - What could we learn from each other".

The Workshop brought together experts from the nuclear, shipping and aviation industries, all three requiring comprehensive regulation and sophisticated technical measures to ensure a high level of safety.

While these industries are different in their nature, in terms of assuring safety they are not as different as it appears. All of those carry an inherent risk to people and the environment. Nuclear power plants do not move, but radioactive clouds cross borders, which underlines the international dimension of nuclear safety issues. In the shipping industry, the traditional approach is to move vessels to areas with 'lighter' regulatory touch. In the aviation industry, the safety requirements (but less so the enforcement) follow agreed-upon international standards.

The conclusion of the workshop was that in all the three industries there is a visible shift from a prescriptive to the performance-oriented regulation to address current and future challenges. In all the industries, the principle of learning from one another to identify best approaches for investigation, analysis, reporting and implementing operational experience is an important element of safety enhancement process.

While recognising a specific regulatory approach that is suited for particulars of each industry, the workshop identified several topics where the exchange of experience could benefit all. Those include the methods and approaches for safety assessment and event investigation, but also regulatory inspection and enforcements practices.

The experts present noted the innovative character of this Workshop and recommended further activities including detailed investigations and follow up on specific topics of common interest. The EC was encouraged to continue its efforts in this respect, by organising future events, starting with topics identified during the 2007 Workshop. The 2012 Workshop was organized in October 2012 with the aim of making further progress in the exchange of views, experience and lessons between the regulated industries.

The project aimed at identifying the safety philosophy and eventual actions that are already flowing across the industries and explore the areas where the cross-cutting activities could be beneficial, primarily for the nuclear sector (as this is the goal of the

© ENCO

project), but also providing the insights and information to other sectors that could lead to an increased safety level of those industries.

1.2 Objectives and scope of the report

Within the project No. ENER/ 2011/NUCL/SI2.599383 (Framework Service Contract for Technical Assistance TREN/R1/350-2008 Lot 3) for the EC DG ENER - Nuclear energy (ENER/D2), the report is intended to present results of the study carried out to investigate the possibilities and merits of cooperation with other potentially hazardous sectors to maintain and further enhance nuclear safety. The report provides a brief overview of practical cases used in this project to illustrate some of the relevant issues as well as summary conclusions from the root cause analysis of these cases.

Three major accidents were selected – one for each of the three industries (N, A, M):

- Tsunami at Daiichi /Fukushima NPP on March 11, 2011
- Crash of Air France Flight 447 on June 1, 2009
- Deepwater Horizon oil rig platform explosion on April 20, 2010

Insights from the analysis of the selected accidents were used to identify possible areas of interest, the strengths and weaknesses of each of the industries, specific issues or weaknesses of safety arrangements as identified by each industry, but also the areas that were identified as in needs of (or candidate for) improvement.

The report also presents the results of the workshop on "How to Improve Safety in Regulated Industries - What Could We Learn From Each Other", organized based on the study mentioned above. The report presents insights obtained and conclusions reached during the Workshop, relating to safety regulation in the nuclear, aviation and maritime industries.

Complete results of the study, as well as information on the organization and conduct of the Workshop is also provided.

1.3 Structure of the report

Section 2 describes the results of the study on the status of the cross-cutting cooperation at present, as well as the outcome of analysis of areas where the cooperation could be beneficial for the future in particular issues where the nuclear industry could learn from the others (and vice versa).

Section 3 describes the organisation and conduct of the workshop as well as the participants of the workshop. This section describes what type of results have been obtained based on the workshop and includes a comparison of the status across the industries and recommendations for future work. The material is structured in terms of specific issues of interest and presented for each of the three industries.

Section 4 provides the main conclusions based on the results of the project.

Annexes A-C provide a detailed overview of major accidents selected for this project.

Annexes D and **E** include the complete list of Workshop participants and the final Workshop agenda.

Annex F provides the PowerPoint slides from the Workshop, including keynote speakers' presentations, as well as the breakout groups' presentations.

2 THE STUDY

Material presented in this section includes some insights from the analysis of the selected accidents which can originate more general ideas in relation to the subject considered in this project. The accidents were chosen to attract the audience and to enable potential Workshop participants to relate to a game-changing environment.

The events are presented at a general level, not going into all the technical details of how the events happened, but rather intended to help in answering the questions like "what could we learn from the events?" and "how to use this to enhance the safety among regulated industries?"

One obvious conclusion is that, at least initially, those high profile accidents could be traced to a lack of “questioning attitude” and maintaining ”business as usual”. This applies both to operators and regulators. It is also clear that the vendors might have some role (e.g. in the AF 447 and Fukushima accidents).

Exploring how each of those could have been prevented by being more vigilant or having a questioning attitude on the side of the regulator and operators, as well as what recommendations where established to enhance a questioning attitude for the future is of interest. Similarly the issue of what kind of role the vendor might play is addressed as well.

Summary insights are briefly discussed in the following subsections, each devoted to specific industry sector.

More detailed overview of major accidents selected for this project is provided in Annexes A – C. These annexes describe the results of causal analysis performed specially for this project. These results are presented in the form of Cause Map (CM) that displays the whole structure of causes in a graphical form. The CM for the selected accidents were developed and presented in MS Excel using the worksheet / template prepared by "ThinkReliability" Consulting Company available at web page http://www.thinkreliability.com.

This form of presentation is believed to facilitate effective communication and documentation of causes of the problem (accident). It is worth noting that communication of findings to experts from different industries and of different professions was an important aspect of this project and that the Workshop participants were provided with the relevant information prior to the Workshop. The documents made available to all Workshop participants were:

- Background material on the Fukushima Dai-ichi Accident,
- Background material on the Deepwater Horizon oil rig explosion,
- Background material on the Air France flight 447 crash,
- Introductory Report summarizing the 2007 Workshop, as well as the study used as the basis for the 2012 Workshop.

The summary of the reports on each of the game-changing incidents in all three industries are listed below.

© ENCO

2.1 Nuclear Sector – Tsunami at Daiichi/Fukushima NPP

Concluding Summary

Technical analysis of the Fukushima Daiichi March 2011 accident [A-1] indicates that the fundamental cause for the severe accident was the loss of substantial systems needed to maintain reactor cooling. The loss of these systems resulted in core damage to reactors at the site and uncontrolled release of radioactive materials to the environment from the site.

From this information and review of the capabilities needed to provide core cooling, it is clear that essentially all plant equipment needed to support core cooling was damaged by the initial effects of the tsunami event.

Other factors outside of the initial effects of the tsunami may have contributed to the extreme challenges encountered in attempts to sustain and/or reestablish cooling; however, the focus of this analysis was on the cause of the loss of the safety systems that would normally be used to maintain the integrity of the core. The loss of those safety systems was a result of a tsunami that exceeded the design basis of the plants.

The tsunami protection strategy for the plant consisted of locating critical equipment, such as vital seawater pump motors, above the elevation of the assessed tsunami height. The plant was constructed in the 1960s and 1970s and the basis for the safety design criteria is unclear. A later assessment of the tsunami height used the 2002 Tsunami Assessment Method for Nuclear Power Plants in Japan, the accepted methodology by the Japanese industry. Following the guidance of this methodology, offshore fault segments were not combined in the tsunami assessment. During the earthquake event numerous fault segments acted in combination, and thus the actual tsunami caused by the earthquake significantly exceeded the tsunami assessment for the plant.

Fundamentally, following the accepted tsunami assessment technical guidance in Japan resulted in under-prediction of the size of the tsunami. As a result, the plant tsunami protection strategy was not adequate and beyond-design-basis tsunami protection adequate to mitigate the effects of the tsunami that occurred was not available.

The Fukushima accidents could have been avoided if the operator had upgraded the plant to reflect today's understanding of the risks and methods used in the evaluation of tsunami [2], [3]. Additional problem was that the regulatory oversight did not force the operators to do so in time, and the Vendor did not provide for the upgrade of the design that reflects the current knowledge.

In addition to that, the operator and the plant were not properly prepared to respond to some beyond design basis accidents that could not be excluded as a low level risk (based on low probability/ low frequency).

General issue of high interest is the development of a concept of protection that would be based on the combination of appropriately balanced defence-in-depth and the risk considerations. Integral element of this concept is the treatment of accident scenarios with low probability and high consequences.

Discussion on accident causes

The technical analysis of the Fukushima Dai-ichi accident traced the cause for the eventual loss of all practical cooling paths for the reactors to the tsunami's flooding of the plant protection. The analysis identified the significant difference between the **design basis tsunami height** and the actual tsunami height, as well as the limitations of beyond-design-basis tsunami protection or mitigation that could address the effects of the actual event.

The tsunami of March 11, 2011 resulted in flooding of plant buildings and submergence of critical SSCs that led to long lasting blackout of the plant. In such situation the plant was not able to provide emergency core cooling in a timely manner that led to the core damage, hydrogen explosion and uncontrolled release of radioactivity.

There were several technical problems that contributed to this accident:

- Limited **capability of batteries** to provide control power needed for accident mitigation.
- Difficulties to provide **emergency power using portable generators** due to limited number of devices available at the site and difficulties with transporting the devices to the plant.
- Difficulties with **manual operation of the relief valve** for depressurization of the reactor system due to the lack of lighting and a high radiation level in the plant compartments.
- Difficulties with **venting the containment** due to the lack of power and compressed air for opening of vent valves (MOV and AOV) and the need to work in a difficult environment.
- Difficulties with the **use of fire pumps** that required non-routine connections to be established in a difficult environment.
- The **lack of indications and controls** of valves involved in the implementation of the required non-routine line-ups.

It is disputable whether the March 11 **tsunami height** should have been expected based on the existing historical evidence. It worth noting that severity of an earthquake that led to this tsunami could have been expected.

The main reason for under-prediction of the tsunami was that the **existing guidance** for the subject (endorsed by the regulatory authorities) did not consider as credible that a tsunami could be caused by ruptures across several fault segments in the vicinity of the plant. The guidance stated that combined fault segments did not need to be considered for faults along the Japan Trench (that encompasses the region of Fukushima). The March 11 earthquake occurred across numerous of the geological fault segments within the Japan Trench, resulting in a tsunami significantly larger-than-expected.

Contributing factor is **unclear regulatory framework** that relies on several organizations with their roles not precisely defined.

2.2 Aviation sector – Crash of Air France Flight 477

Concluding Summary

AF 447 problem involved a combination of training/procedure problems and the specifics of the design, both of which could have been identified and questioned, leading to changes that could possibly have prevented the accident [4].

Vulnerability of speed sensors (Pitot tubes) should have been recognised based on previous incidents, but the problem was not resolved in time [5]. Failure of this type should also be reflected in the training of flying crews. On this the Vendor's communication with the Operators' training/safety department might be questioned.

Important issue is the increasingly automated nature of modern aircraft and potential problems when flight management systems fail. Under these conditions pilots may not have the information they need to save the plane. The technological sophistication of

modern aircraft may also mean that new pilots are no longer well trained in flying without the assistance of modern gadgetry.

Discussion on accident causes

Technical analysis of the accident identified several causes of the crash of AF447 flight which can be controlled by the problem owner. These include weaknesses related to design, procedures and training.

Report from air crash investigators [4] revealed a common cause **failure of the plane's speed sensors** (plugged by icing) – critical for fly-by-wire computer-assisted flight - followed by the flight crew inexplicably failing to maintain airspeed and deal with the plane stall that resulted from this failure.

Important contributor to the failure of the crew to handle the plane stall conditions was the **lack of information on the angle of attack**, which in the current Airbus design is not directly accessible to the pilots. This information would enable crews to identify the aerodynamic stall conditions in a law other than normal law when the automatic pilot and most of automatic protections are not available. Under these conditions, manual handling can bring the airplane to high angles of attack such as those encountered during the AF447 event. It is essential in order to ensure flight safety to reduce the angle of attack when a stall is imminent. Only a direct readout of the angle of attack could enable crews to rapidly identify the aerodynamic situation of the airplane and take the actions that may be required.

Several causes are closely related with the **crew resource management**. They include:

- Task-sharing not defined by the captain
- Co-pilots did not brief the Captain on his return
- Left and right controls not linked.

The investigation showed that an absence of training and practice for a crew consisting of two copilots does not guarantee a level of performance equivalent to a crew consisting of a captain and a copilot when faced with a degraded situation. The absence of a hierarchy and of effective task-sharing in the cockpit strongly contributed to the low level of synergy. The anxiety generated by the absence of the captain from the cockpit shows that the two copilots were not capable of resolving the emergency situation initiated by the failure of flight automatics. This can be explained both by the absence of any **appropriate training** and a **lack of decision-making practice** on the part of the two copilots.

First two causes indicate problems with **cockpit procedures and weaknesses of the pilots' training programmes**. Enhancement should focus on clear definition of criteria for the role of relief captain and ensuring better task-sharing in case of relief crews.

Delinking the left and right controls of AB-330 was a **design feature** that contributed to the critical sequence of events leading to the AF447 catastrophic outcome. In a plane with the right and left seat controls linked, the Pilot Not Flying (PNF) would have been able to detect mistaken decision Pilot Flying (PF) to lift the plane’s nose and correct it. It is worth noting that the Airbus designers delinked the 330’s controls, which made it possible for PNF to remain unaware of PF’s error until it was too late to fix.

The pilots training scheme implemented by AF is **lacking a comprehensive training** on avoiding stalling and recovery from the stall conditions at cruise altitude. High altitude stall training in the simulator has to be emphasized, along the other lessons required.

The investigations of AF447 crash also showed that the **experience feedback process** in place at Air France needs improvement. Analysis of incidents and near-misses should be

conducted with a more careful consideration of potential risk aspects. Decisions on the implementation of appropriate correction actions need to be risk informed. It is evident that the risk of an accident comparable to the AF447 crash (in the light of the existing operational experience) has been underestimated and appropriate actions that would prevent severe accident have not been implemented in time.

Operating evidence indicates that the likelihood of Pitot probes icing was relatively high. At the same time deficiencies of the training programme related to plane stalling conditions and stall recovery at cruise altitude makes the likelihood of the catastrophic outcome not negligible. If such evaluation had been conducted the appropriate corrective actions would have been implemented in time to prevent the AF447's disaster.

2.3 Maritime/offshore sector - Deepwater Horizon oil rig platform explosion

Concluding Summary

The Gulf oil spill might have been prevented by having a stronger safety culture (or questioning attitude) at the rig and more thorough regulation and oversight.

Majority of issues identified in the accident investigation are rather specific to the technology of deepwater oil drilling. They should be carefully addressed by the industry (operators, drilling contractors and service companies) and resolved through appropriate changes in the procedures and training programmes. Regulatory agencies have also important role in enforcing appropriate changes.

However, most of the issues can be traced back to underlying causes of more general type, such as management system, safety culture, and safety oversight. Some of them can be of general interest to different industries and are worth to be discussed during the workshop.

Comparisons have to be made and conclusions drawn with care, taking into account significant differences of industries considered in the project. It is important to note that the deepwater oil drilling industry is rather specific area that involves a large number of facilities and was subject to intensive development of technology and rapidly expanding production activities.

The Macondo blowout was the product of several individual missteps and oversights by BP, Halliburton, and Transocean, which government regulators lacked the authority, the necessary resources, and the technical expertise to prevent. The extent to which each of these missteps and oversights caused the accident to occur will never be precisely known.

What we nonetheless do know is considerable and significant:

(1) Each of the mistakes made on the rig and onshore by industry and government increased the risk of a well blowout;
(2) The cumulative risk that resulted from these decisions and actions was both unreasonably large and avoidable; and
(3) The risk of a catastrophic blowout was ultimately realized on April 20 and several of the mistakes were contributing causes of the blowout.

Deepwater drilling is an inherently risky business given the enormous pressures and geologic uncertainties. It is now clear that both industry and government need to reassess and change business practices to minimize the risks of such drilling. Findings of accident investigations highlight the importance of organizational culture and a consistent commitment to safety by industry, from the highest management levels on down.

But that complacency affected government as well as industry. There were weaknesses and the inadequacies of the federal regulation and oversight that require changes in legal authority, regulations, investments in expertise, and management. Resources of the regulatory agency (Minerals Management Service) did not keep pace with industry expansion into deeper waters and industry's related reliance on more demanding technologies. And, senior agency officials' focus on safety gave way to efforts to maximize revenue from leasing and production.

Discussion on accident causes

The most significant failure at Macondo-Deepwater Horizon rig – and the clear root cause of the blowout – was a **failure of industry management**. Most, if not all, of the failures at Macondo site can be traced back to underlying failures of management and communication. Better management of decision making processes within BP and other companies, better communication within and between BP and its contractors, and effective training of key engineering and rig personnel would have prevented the accident.

BP's **management process** did not adequately identify or address risks created by late changes to well design and procedures. BP did not have adequate controls in place to ensure that key decisions in the months leading up to the blowout were safe or sound from an engineering perspective. It should be noted that changes to drilling procedures in the weeks and days before implementation were not subject to any peer-review or management of change (MOC) process. At Macondo, such decisions appear to have been made by the BP Macondo team in *ad hoc* fashion without any formal risk analysis or internal expert review. This appears to have been a key causal factor of the blowout.

Halliburton and BP's **management processes** did not ensure that cement was adequately tested. Halliburton had insufficient controls in place to ensure that laboratory testing was performed in a timely fashion or that test results were vetted rigorously in-house or with the client. In fact, it appears that Halliburton did not even have testing results in its possession showing the Macondo cement slurry was stable until after the cementing job had been completed. It is difficult to imagine a clearer failure of management or communication.

The story of the foam stability tests may illuminate **management problems** within BP as well. More than two weeks before the accident, BP team members had recognized the importance of timely cement testing and identified concerns regarding the timeliness of Halliburton's testing process. But despite their recognition that final changes to the cement design might increase the risks of foam instability, BP personnel do not appear to have insisted that Halliburton complete its foam stability tests and report the results to BP for review before ordering primary cementing to begin.

BP, Transocean, and Halliburton **failed to communicate** adequately. Many BP and Halliburton employees were aware of the difficulty of the primary cement job. But those issues were for the most part not communicated to the rig crew that conducted the negative-pressure test and monitored the well. It appears that BP did not even communicate many of those issues to its own personnel on the rig. Transocean failed to adequately communicate to its crew lessons learned from a similar near-miss on one of its rigs in the North Sea four months prior to the Macondo blowout.

Management and communication issues mentioned above clearly indicate **problems with safety culture**. Resulting from a deficient overall system approach to safety is evident in the multiple flawed decisions that lead to the blowout. These problems involved the lack of management commitment to safety, lack of the questioning attitude and safety awareness, insufficient level of knowledge of procedures and rules and lack of operating

discipline, incompliance with the existing internal procedures or work practices, and inadequate communication on safety matters between individuals and groups.

BP was aware of problems with Halliburton personnel and work product years before the blowout. Despite that BP's own well site leaders accepted facially implausible explanations for results of the negative test. BP's on-duty well site leader was not even present during preparations for the critical negative pressure test, and may not have been present during the beginning of the negative pressure test itself. In the light of these facts, the management commitment to safety is questionable.

Decision making processes at Macondo well did not adequately ensure that personnel fully considered **the risks created by time- and money-saving decisions**. None of such decisions appear to have been subject to a **comprehensive and systematic risk-analysis**, peer-review, or management of change process. The companies are lacking of appropriate organizational and technical framework for a systematic risk assessment, or if such framework existed, it was not in use.

BP team decision of not conducting a **cement evaluation log** did not fully conform to the intent of its own guidelines. Introducing *ad hoc* changes in the temporary abandonment procedure at Macondo also indicates **procedure-related problems** at BP. That procedure changed many times during the week leading up to the blowout without any assessment of the related risks.

Learning from operational events or near-misses was minimal or non-existing. Also the **use of existing expertise and knowledge** within the corporation and sharing knowledge between members of the rig crew was not effective.

2.4 General insights and conclusions from the selected case studies

The following important issues can be formulated based on the case studies:

- **Communication** within the Safety Net[1] is an issue that requires increased attention. In some cases Vendor's communication with the Operators (training/safety department) might be questioned. Regulators' response to the identified safety issues also requires improvement (e.g. Fukushima case).
- The role of **self-assessment, questioning attitude and safety culture** are important issues that require increased attention and in many cases need improvement (e.g. Deepwater Horizon case).
- **Operating experience feedback** at the company level and Safety Net level as well as international (supranational) level requires improvement (e.g. AF447 case and Deepwater Horizon case). Some symptoms of negative impact of globalization, deregulation, and associated market pressure on the safety can be observed based on the practical case studies (e.g. AF 447 case and Deepwater Horizon case)).
- Concept of **continuous improvement** based on proactive approach that use operational feedback from minor incidents and near-misses at the company level needs to be strongly recommended. There are some indications of the lack of proper response to such events (e.g. AF 447 case and Deepwater Horizon case).

[1] The term SAFETY NET is used in this report to describe collaborative, mutually-supporting activities of entities sharing responsibility for safety within an industry (see Section 4 for more details).

- **Training programs and procedures** needs to be well co-ordinated with the specific design features that reflect modern technology (such as the increasing role of digital technology, automatics in safety related systems). Some problems of this type can be observed based on the practical case studies (e.g. AF 447 case).
- **Safety oversight** based on prescriptive regulations demonstrated the need for changing the existing system for a proactive goal-oriented system integrating all aspects of operations that could affect occupational and process safety. The new regulatory system should incorporate a limited number of prescriptive elements into a proactive goal-oriented risk management system for health, safety and the environment (e.g. Deepwater Horizon case).

The above-mentioned topical issues served as a basis for the 2 day Workshop which took place in Luxembourg in October of 2012. The Workshop brought together European key players from the three sectors in order to exchange views on the implementation and lessons learned regarding all the aspects highlighted in the study. The details of the Workshop are described in the following section.

3 THE WORKSHOP

An important finding of the "2007 Cross cutting workshop" was that there are specific approaches, methods or arrangements of interest to be transferred across industries. Several specific areas were identified, mainly those related with the human factors and procedures, man-machine interfaces and alike - issues every industry has been facing on its own.

The workshop also confirmed that none of the industries represented at the workshop is unique in facing safety issues but the methods of addressing these are different in different industries. Exchanging views and experience between the aviation, shipping and nuclear industries was considered of great value for all three industries.

All industries that have potential for affecting the environment and humans operate independently from each other, without overlapping of business activities and/or commercial interests. Thus, it is believed that there should be no obstacles to sharing experience and insights and/or methods and approaches that might lead to a higher safety level across industries. In this way, building upon the success of the 2007 "Cross Cutting Workshop", this project attempted to identify the safety philosophy and eventual actions that are already flowing across the industries and explore the areas where the Cross Cutting activities could be beneficial, primarily for the nuclear sector (as this is the main activity of the EC department that launched this project), but also other industries that are participating in it. It aimed at providing insights and information that could lead to an increased safety level of those industries.

It is the EC's interest to see whether any successful co-operation could be established and what would be the priorities and the topics of this co-operation. In this respect, the 2012 Workshop aimed to determine what would be this area, how to establish the cooperation and what could be the EC's role in it.

3.1 Objectives

The objectives of the workshop included:

- To bring together regulators, operators and vendors from all three industries (A/N/M) and discuss their experiences in co-operation with the other sectors,
- To investigate the causes and roles of major "game changer" safety events (Fukushima accident, Deepwater Horizon Gulf oil spill and the Air France flight 447 accident),
- To investigate common themes of interest across the three industries,
- To highlight practices which have proven to be efficient and effective,
- To identify particular areas were cooperation should be further developed,
- To identify potential new areas of cooperation,
- To identify possible measures to improve the situation in the nuclear sector at the EU level,
- To establish recommendations for the EC DG ENER for future initiatives.

3.2 Scope

In order to identify important differences, similarities and best practices across the A/N/M industries, the workshop addressed several areas of interest:

- Causes and outcomes of major game-changing events in all three industries
- Discussion of keynote safety challenges
- Importance and possibilities of Communication within the Safety Net
- The role of self-assessment, questioning attitude and safety
- Operating experience feedback at the company level and Safety Net level, as well as international (supranational) level
- Exploring the role and importance of challenging attitudes among actors in all three industries

3.3 Participation

The Workshop brought together representatives from 18 countries and 6 international organisations. The participants represented a wide spectrum of experts from all three industries, from top managers of international and national organizations dealing with safety to industry experts with long experience in safety issues. Most of the participants are personally involved in the safety assessment and/or safety engineering in their respective industries.

The list of participants is provided in Annex D.

3.4 Workshop organization and conduct

Based on the review and consultation with DG ENER and based on the study conducted as part of this project, a list of organisations and experts to be invited was compiled.

In designing the structure and the agenda of the workshop a number of considerations were taken into account:

- The need for participation from vendors, operators and regulators (V, O, R) from all three industries was considered beneficial. While in the nuclear field safety is exclusively the responsibility of the operator, in aviation the designer/vendor shares a considerable part of this responsibility, and exploring these differences would help in identifying roles in establishing and maintaining the safety net. The vendor/designer, regulatory and operator's perspectives should be taken into account. The term SAFETY NET is used in this report to describe collaborative, mutually-supporting activities of entities sharing responsibility for safety within an industry. Within this there is a common goal, but complementary approach (focus). Responsibilities are overlapping but at the same time redundant (in the sense that specific tasks might be implemented by one or another of the players –the players being V, O, R). A more precise definition of the "NET" was discussed during the Workshop.
- The vertical (N, A, M sector) or horizontal (V, O, R actor) structure of the workshop and agenda was also considered. In the discussion it was concluded that the vertical approach still has more benefits. Issues of understanding could have arisen from the horizontal approach.

Agenda of the workshop is provided in Annex E.

Topical issues were formulated and speakers for the invited keynote lectures were selected.

The workshop was structured to provide industry-specific insights to all the participants. 17 keynote contributions were structured in 7 topical sessions. The topics addressed were:

- Game-changer events, analysed by non-parties,
- The Safety NET concept,
- Keynote safety challenges in all three industries,
- Supranational frameworks,
- Experience in cross-cutting.

This established a basis for comprehensive discussion leading to the formulation of conclusions.

The presentations of all of the keynote speakers are included in Annex F of this report.

The second day of the workshop was devoted to working in the groups. Topical discussions were held in four breakout sessions, followed by a general discussion that helped with formulating general conclusions. To facilitate this task, specific topical issues were defined that were intended to provide a suitable logic for the discussions. The four breakout groups discussed the following issues:

Group 1: How to establish a challenging attitude to enhance safety?; Drivers and the roles in achieving, maintaining and strengthening safety

Group 2: How to strengthen the safety NET?; Interaction of vendors, operators and regulators, confrontation vs. collaboration, role of supranational regulation

Group 3: What is the impact of major events on safety thinking/concept – are those game changers?; Lessons for vendors, operators and regulators

Group 4: What can we learn from each other?; Practical aspects and learning field from other industries, what is "transferable" and what not

These topical issues are further discussed in section 4.1.

Moderators and group leaders with high professional standing and a long time experience were appointed for each session. In the final session of the Workshop, the conclusions of the breakout groups were presented and recommendations formulated.

4 OVERVIEW OF THE OUTCOME AND WORKSHOP CONCLUSIONS

4.1 Topical issues addressed by the working groups

Challenging attitude within an industry

The group was intended to discuss challenging attitudes within the industries – its drivers, its role in achieving, maintaining and strengthening the SAFETY NET. Aspects related to financial pressure (operational costs, loss of assets, etc.), public perception and their impact on safety are covered in this group.

The group discussed the issue of how to create/enhance a challenging attitude and the role of a challenging attitude in strengthening the safety net. Some of the group's conclusions are listed below:

- Fostering an effective challenging attitude is a role of all stakeholders. There are different roles, but all them must be aligned - dialogue is key.
- This can be achieved extrinsically ("push") or intrinsically ("pull"). The second option is more effective and more sustainable. However, both are extremely important. There is a "natural" tendency to focus on the extrinsic one. It is important not to fall into the trap of using only the extrinsic approach, because it will be difficult to overcome it later.
- In achieving an effective challenging attitude several elements play a significant role:
  - Leadership (at all levels) in organizations. How they model, reinforce, coach the proper behaviors of a challenging attitude. This requires specific training and development that not all leaders have. They have to be able to instill a sense of uneasiness, of mindfulness.
  - Sound processes for organizational learning (data collection and actions derived), taking safety into account in the decision process, training of people to ensure that they are mindful about safety, and many more. These are elements of a Safety Management System.
  - Regulators and other stakeholders must create an environment conductive to a challenging attitude. It is considered that a performance-based regulation can help enhance a challenging attitude in the responsible organizations.
  - While maintaining learning from what is wrong, we need to learn more from what is working well (resilience engineering, appreciative inquiry, etc.).

Enhancement of a "Safety Net"

The group aimed at discussing the understanding of the safety net and the individual roles of vendors, operators and regulators in it. The role of self-regulation was one of the important issues addressed in this group.

The group's conclusions are summarized below:

- Definition of safety net: All measures and technical and administrative controls taken by all actors to prevent identifiable risk - from manufacturing of components, design, operation, maintenance up to enactment, implementation and enforcement of national regulations and international instruments and supervision.

- The ingredients of a strong safety net:
  - Clear responsibility assignment and accountability of the various actors
  - Binding safety standards, continuously improved and effectively implemented and enforced
  - Development of safety culture within each organization (including reporting and analysis of near misses, precursors, incidents)
- The establishment of a Safety Net should represent a combined effort of all stakeholders at each of the three safety net layers – industry, national regulators, supranational organizations
- The Safety Net could be promulgated within an organization though:
  - Establishment and effective implementation of a safety policy within the organization
  - Operating experience feedback
  - Continuous hazard identification
  - Clear communication of safety policy and roles

Impact of major events

The group discussed the impact of major events and whether they can be seen as game changers. Lessons for vendors, operators and regulators were also discussed, as how to best make use of their visibility, consequences, public awareness, etc.

The group concluded the following:

- Major events are important for paradigm changes
- The paradigm now is that severe accidents can occur, but are not acceptable and everything must be done to avoid it and its consequences
- Usefulness in learning from near misses as well, not only major events
- Importance of highlighting the non-existence of zero risk – attention should be paid to low consequences
- Importance of communication the benefits of the vendor's, operator's and regulator's activities
- Importance of adapting – a continuous work which needs a continuous and dynamic approach
- Stressing the need for Periodic Safety Reviews and Peer Reviews
- All industries can learn from others and must do so, in respect to events, solutions and implementation trajectories

Learning from experience

The group discussed practical aspects of learning from operational experience and identify potential learning fields within the Safety Net. The issue covered was the learning from other industries and what is "transferable" and what not.

Some of the group's conclusions are listed below:

- Which issues are “universal“ and which specific:

  High level principles and approaches

  - Resource management
  - Safety focus and its elements

  All professional knowledge

  - Analytical methods, risk-based approaches
  - System for feedback of operators’ experience
  - Safety culture, HF and organizational factors
  - Scientific approach in the effectiveness of regulation

  Middle level likely too industry-specific

  - Data and analysis
  - Applications resolving industry-specific issues (CRM in aviation)
- Is transferring lessons/practices worthwhile:
  - Generally yes, but the conditions should be right (National audit scheme - IMO learned from ICAO, oil installations and rigs used CRM concepts from aviation, but developed own application around it)
  - Scientific concepts/principles are worthwhile
  - Custom-made solution are likely not
- What are enhancing and hindering factors:

  Enhancing factors:

  - Achieve understanding of other industry before investigating
  - Looking from perspective of own industry
  - Questioning attitude

  Hindering factors

  - Legal requirements, insurance (on accidents)
  - Lack of motivations (compartmentalized thinking)
  - Industry-specific language, acronyms, large volume of info
  - Not knowing what other industries are doing

  How to organize the exchange?

  - Difficult - focus on specific items where people use same language
- Framework to foster/promulgate transfer:
  - Currently no industry-wide framework exists
  - Communication driven by industry-specific issues
  - Focus on own work, little idea what others are doing
  - Not clear what benefits it would bring

© ENCO

- Need to bring together e.g. regulators from various industries to obtain insights into what others are doing

The PowerPoint presentations summarizing the conclusions of all four breakout groups are included in Annex F of this report.

4.2 Conclusions

Even though the Workshop was organized on the background of three highly visible accidents – the loss of Air France 447, the Deepwater Horizon oil spill, and Fukushima meltdown, the discussions were, however, not limited to these accidents and included issues that were relevant both within and between the three industries (aviation, off-shore, and nuclear), as well as for other safety critical industries. The conclusions listed below summaries the discussions of the Workshop and final conclusions reached as a result of these discussions.

4.2.1 The Inevitability and Perception of Risk

The public's perception of risk is an important factor. It is an undeniable fact of life that accidents occur and always will occur and that a few of these accidents will be severe. While the notion of zero risk or absolute safety may be politically attractive, anyone who has ever worked with safety issues knows that this is a goal impossible to achieve. It is important to acknowledge that fact on all levels of society. The public is understandably attracted by the notion of 'zero risk' and politicians may sometimes be tempted to make promises they cannot keep. It may also be difficult for the lay person to understand the scientific and philosophical arguments against 'zero risk'. This makes it all the more important that the communication between specialists and the public (including the politicians) is made in a clear and effective manner.

While each industry can and must learn from the incidents and accidents that happen to them, each industry must also learn from the incidents and accidents that happen to others. Yet, both intra-industrial and inter-industrial learning could be a lot more effective. For some industries, such as aviation, the intra-industrial dissemination of knowledge seems to work acceptably well, while for others considerable progress still needs to be made. And as far as inter-industrial learning is concerned, there are few examples of this being done well, despite the obvious importance.

4.2.2 The Role of Regulation

One way in which learning shows itself is in the regulation of an industry. The regulator clearly represents an important form of intra-industrial learning, although often limited to a country, region, or culture. The approach to regulation also seems to be specific to an industry. Aviation clearly moves in the direction of more performance and incentive based regulation, while nuclear – in Europe - seems to be going towards stricter and more rigid prescriptive standards, although some countries had implemented partially performance-based regulation. Perhaps the only common feature is that regulators need to 'talk softly but carry a big stick', and have at their disposal effective means to draw the line on wayward operators.

In terms of how regulation is carried out in practice, there are characteristic differences among the industries. In aviation, much of the safety thinking lies with the vendors – no doubt because the product (the airplanes) is highly standardized and because there only are very few manufacturers/vendors worldwide. In nuclear, the ultimate responsibility for safety is with license holder (utility). Another reason for such differences may be that while some industrial systems are unmovable (nuclear power plants, stationary off-shore units land-based industries in general), others not only can be moved but are by design made to be moved, such as airplanes, mobile off-shore units and ships. For the latter some form of global regulation is necessary, since the operation of the system is not fixed to a specific location. Even in the case of nuclear, some kind of global regulation is necessary, since the consequences of an accident (release of radioactive materials) can have an impact far away from where the accident happened. (The same, of course, goes for most other industries, pharmaceutical, chemical, and agricultural in particular.) Vendors may also have a vested interest in global standards, since this makes it possible to sell their technology across the globe. That goes for nuclear, aviation, off-shore, and maritime alike.

4.2.3 Learning – The Transfer of Experience Between Industries

There are many specific areas where industries could learn from each other, some obvious and some less so. Learning, in the sense of the transfer and transformation of experience, is however neither simple nor fast. The easiest way to learn seems to be a transfer either at the level of general characteristics (framework or programmatic level) or at the level of methods and theories (safety analyses and the general assumptions about why accidents happen). Learning is especially transferable at the level of Human and Organizational Factors, including leadership and culture influence on safety.

There are, however, also potentially serious hindrances to transfer both within and between industries. In the case of the latter, it often seems to be the case that one industry lacks information about the approaches and methods use by another industry. Conferences and knowledge transferring events are typically industry oriented, and even in the more general scientific conferences each industry will be allocated to specific tracks or sessions. Another serious hindrance is the lack of time (rather than motivation) and the lack of understanding that comes from differential use of specialized vocabularies (terminologies).

There are nevertheless substantial gains to be made by learning from the experiences in other industries, specifically when particular solutions or techniques can be 'transplanted'. One such example is Crew (or Cockpit) Resource Management (CRM), which was developed in aviation but which has been adapted for use in both maritime (Bridge Resource Management) and offshore. Other issues such as how to write effective emergency procedures have been studied extensively by the nuclear industry (for example, symptom based versus event-based procedures), and the lessons learned from that might possibly be applied in other domains.

Additionally, possible lessons the nuclear industry could learn from the aviation industry would be:

1 Identify the critical elements of a nuclear oversight system and establish a certification process which suites your needs;
2 Measure the maturity of each operators and State oversight system;
3 Act accordingly and differently based on those maturity levels.

4.2.4 Ideas for Further Development

The three industries are in many ways fundamentally different and it is, therefore, not surprising that they have developed in different ways. Aviation seems to be leading with a prudent regulatory approach, and also with industry-wide cooperation. The results (in terms of a reduction in the number of accidents) show that it has been working well so far. Extensive cooperation among vendors, operators and regulators (national and international) also seem to play an important role. Other industries could possibly learn from each other, but the transfer of experience is neither easy nor wholesale, and should not be undertaken without first making sure that the differences between the domains are manageable.

Everyone benefits from increased safety, the industries as well as the public. While there is agreement on the ultimate goal, there is some debate on the best way to get there. Some advocate unified regulation and standards, other flexibility and self-ruled competence, and some a culture of mutual trust. Finding an effective set of ways to improve safety is obviously a joint interest for the public, for vendors, for operators, and for regulators.

The discussions at the meeting brought forward a number of suggestions for what could be done in practice across industries.

- Establishing a questioning attitude and keeping an open mind. This is clearly valuable for each industry as a prerequisite for enhancing safety. A questioning attitude will make it easier to identify areas for improvement. It should also be applied between industries, so that one looks for good solutions everywhere.
- Performance based regulation. This kind of regulation embodies the questioning attitude, since it is requires that everyone continually looks for the best solutions and ways of performance improvements. In order to implement this in practice, regulators need to have a strong independent position as well as strong technical capabilities. Performance based regulation can be supported in various ways, for instance by thorough peer reviews (or audits), periodic safety reviews that focus on good practices, etc. Performance based regulation may lead to an increased peer pressure and increased demands for achieving excellence. Important to note is, however, that peer reviews – although having the potential to be of great value – can also sometimes lack objectivity. Independence is, therefore, important and valuable and there might also be a need for a new kind of inspector – one capable of a more holistic approach and one less driven by mere compliance.
- Looking for cross-cutting diversity. Every industry excels in something, depending on its historical development. The strengths of an industry should be identified both at a program/concept level and at specific technical levels. They should be explored further, in order to be clear about what is required before they can be applied in a different setting.

5 ACTION POINTS

As a result of the study conducted and the workshop organized within the scope of this project, the following action points were developed as to identify possible measures to needed to improve the situation in the nuclear sector at the EU level.

One important role of the EC is to encourage the discussions where the problems, experiences, and solutions could be exchanged across industries. This could be done with regard to a number of issues, some of which are listed below.

Regulations:

- Improved cooperation among EU regulators in the three industries (aviation, nuclear maritime); *[A consideration on possible future cooperation between industries could extend to the European Defense Agency (EDA), as well as the European Agency for Safety and Health at Work (EU OHSA), European Railway Agency (ERA) and European Chemicals Agency (ECHA)]:*
  - The efficiency of regulation, relative to the different regulatory structures;
  - The potential of performance based regulations in all industries.
  - How to achieve the proper balance between clarity (of regulation) and the industries' need to manoeuvre.
- Absolute safety versus relative safety; acceptability of risk from various standpoints, and the concept on residual (tolerable) risk, and consideration of tolerability of risk across industries.
- Practice of undertaking international or peer's audits, on both regulators and operators; optimal way of organising audits.
- While maintaining learning from what went wrong in other industries, reinforce the use of opportunities for learning from what went right or excellent.

Specific exchanges on the topics of interest (eventual future workshops/exchanges):

- Human factors and organisational safety issues
- Procedures (normal and emergency, event based, symptom based) and their designated uses
- Improving the preparedness for unforeseen events; How to train operators to act in cases where there are no instructions given operators' resource management
- Effective use of operational experience, event analysis and lesson learned (*retour de l'experience)*
- Early identification of "faint signals" in order to correct problems when they are still small
- Cost-effectiveness of measures to improve safety, in the near-, mid-, and long-term. Effectiveness of implementation of measures
- The consequences of aging – of hardware, software, people and organizations, knowledge

6 REFERENCES

[1] "Workshop on Cross Cutting Comparison of Regulation and Operation of Industries Requiring Specific Safety Rules - Summary report", ENCO FR-(07)-32, prepared for EC TREN H2, October 2007.

[2] "*Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station*", No. INPO 11-005, Revision 0, November 2011.

[3] EPRI, "*Fukushima Daiichi Accident – Technical Causal Factor Analysis*", Report # 1024946, Final Report, March 2012.

[4] SWISS FEDERAL NUCLEAR SAFETY INSPECTORATE ENSI, "In-depth Analysis of the Accident at Fukushima on 11 March 2011 With Special Consideration of Human and Organisational Factors, Report #11032011.

[5] "3rd Interim Report on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris", Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile, Ministère de l'écologie, du développement durable, des transports et du logement, Rev 3 (29 July 2011).

[6] BP, Deepwater Horizon Accident Investigation Report, September 8, 2010.

[7] "*Deepwater, The Gulf Oil Disaster and the Future of Offshore Drilling*", Report to the President, National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, January 2011.

© ENCO

7 Annex A. Overview of Fukushima Daiichi Accident

A1. Accident Summary

On March 11, 2011, the Fukushima Daiichi nuclear power plant experienced a seismic event and subsequent tsunami.

The initiating seismic event involved multiple ruptures of seismic sources over an area of about 250 miles x 125 miles. The earthquake was very significant (magnitude ~9), considered the fourth largest in recorded world history. Although the earthquake did not cause significant structural or operational damage to Fukushima Daiichi, the event did cause major infrastructure damage to areas around the plant. The offsite damages led to loss of offsite power.

The earthquake caused a series of tsunamis, the largest of which arrived at Fukushima Daiichi approximately 41 minutes after the earthquake, reaching a wave height of approximately 15 m. The associated volume of water – and the related hydrodynamic forces – caused extensive and deep flooding in and around all major structures of operating Units 1 through 3 that led to a loss of on-site power and subsequent loss of all core cooling systems. The loss of these systems resulted in core damage to reactors at the site and uncontrolled release of radioactive materials to the environment from the site.

The design basis seismic definitions were – in magnitude and frequency content – not significantly different than the actual seismic event. However, the nature of the seismic event (that is, occurring across a large area and involving multiple ruptures of seismic fault segments) was not incorporated into the design basis tsunami definition.

The accident and the ensuing mitigation and recovery activities occurred over several days, involved a number of incidents, and might provide several opportunities for lessons learned.

A2. Causal analysis

Step 1 - Definition of the problem

The first step of the Cause Mapping approach is to define the problem by asking the four questions: What is the problem? When did it happen? Where did it happen? And how did it impact the goals? Answers to these questions are provided in the following table.

What	Problem(s)	Fukushima/Daiichi tsunami
When	Date	March 11, 2011
	Time	
	Different, unusual, unique	Large earthquake/ tsunami;
Where	State, city	Fukushima, Japan
	Facility, site	Daiichi nuclear power plant
	Unit, area, equipment	Units 1 - 3
	Task being performed	Operating at full power

Impact to the Goals

Safety	11 workers injured
Public Safety	Potential for health impacts
Environmental	Release of radiation to the environment
Customer Service	Evacuation of public within 20 km
	Rolling blackouts
Production - Schedule	Loss of electrical production capacity
Property, Equipment, Mtls	Catastrophic damage to plant
Labor, Time	Massive efforts to cool reactor

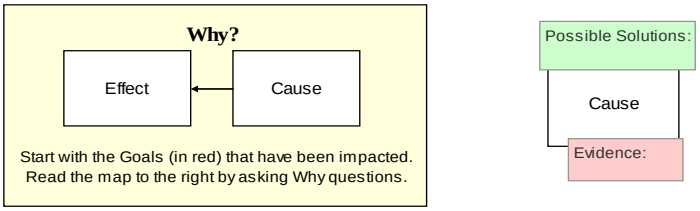
© ENCO

Frequency Very rare

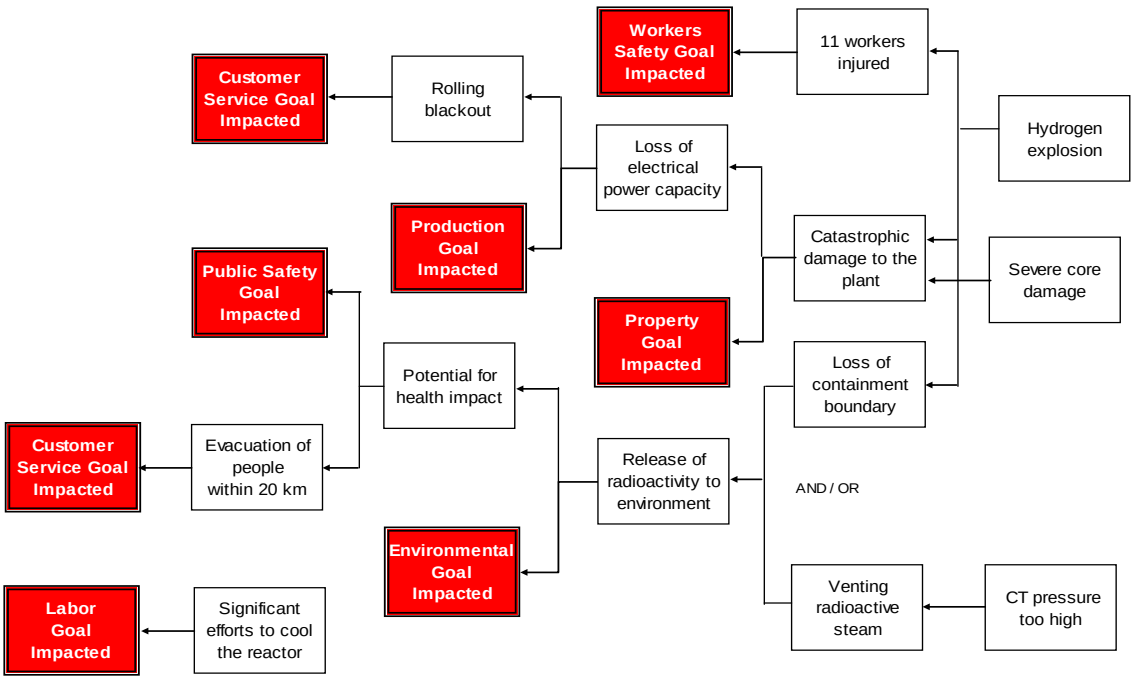
Step 2 – Analysis of causes (Causal Map)

Catastrophic damage to the plant was caused by the hydrogen explosion and severe core damage. Release of radioactive material to the environment was caused by venting of the containment and in the later phase of the accident by the loss of containment boundary due to hydrogen explosion in the reactor building.

Venting of the containment was undertaken in order to decrease the containment pressure that was too high. Buildup of the containment pressure was caused by the lack of containment cooling and heating of the containment. Without heat removal systems (no AC power and a loss of ultimate heat sink), containment pressure and temperature increases as energy from the reactor is transferred to the containment via safety relief valves (SRV) or systems such as RCIC and HPCI.



Step 2. Cause Map - Page 1



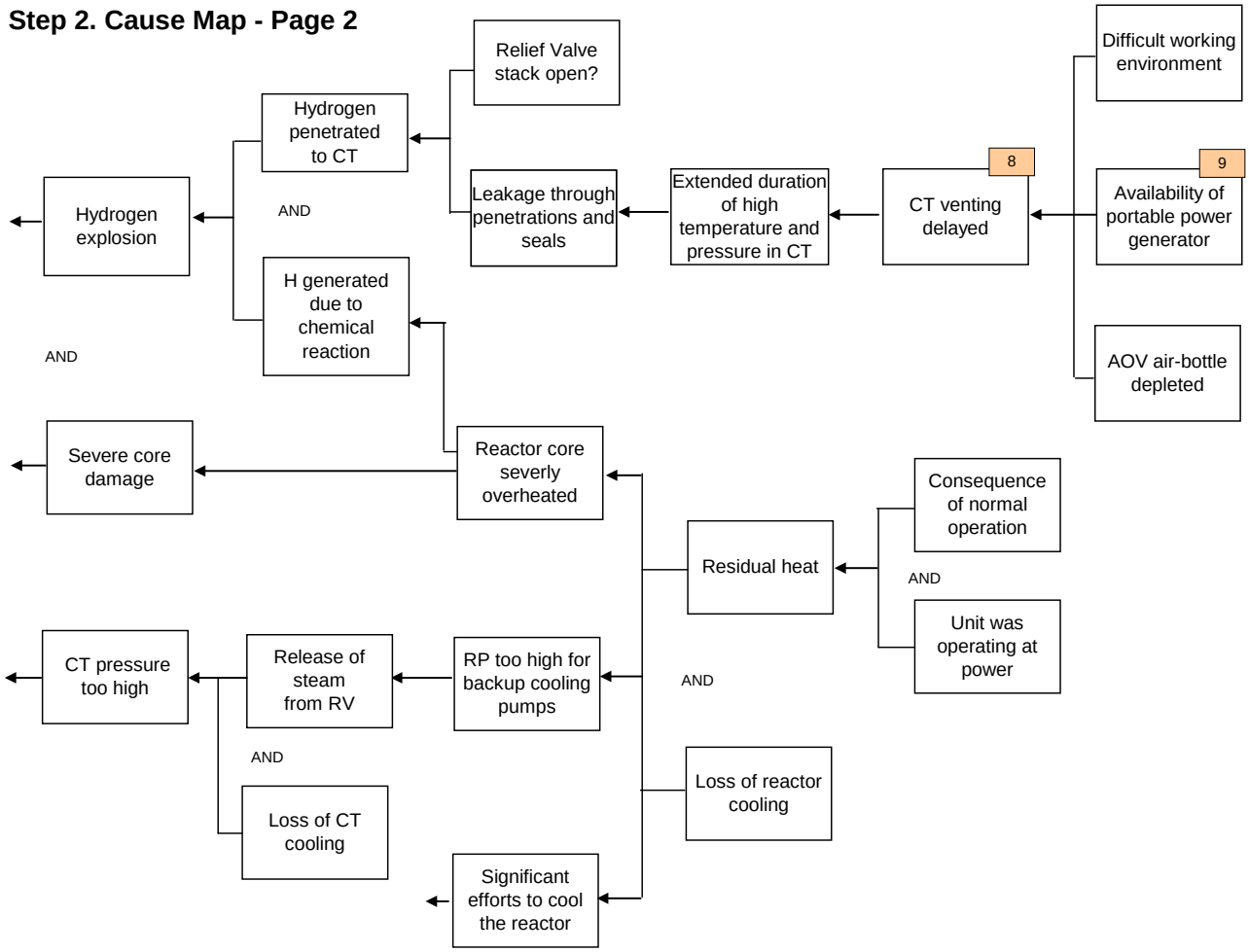
Following loss of RCIC and HPCI, the release of steam from the reactor system via SRV was performed by the personnel in an attempt to depressurize the system. Reactor pressure was too high and had to be reduced to allow injection using a fire pump – at this moment the only available means to maintain the reactor vessel water inventory and to prevent uncovering of the reactor core. Depressurization of the reactor system was achieved by releasing steam through the relief

valve that was open manually by the personnel. This action was difficult to achieve due to a high radiation level and the lack of lighting in the plant compartments.

Opening of vent line required electric power to energize the valve solenoid for the large air-operated suppression chamber vent valve that was done using a small portable generator. Completion of this work required also replacing the temporary air bottle for the AOV vent. These actions took about 4 hrs and contributed to the delay in providing water injection to the reactor system.

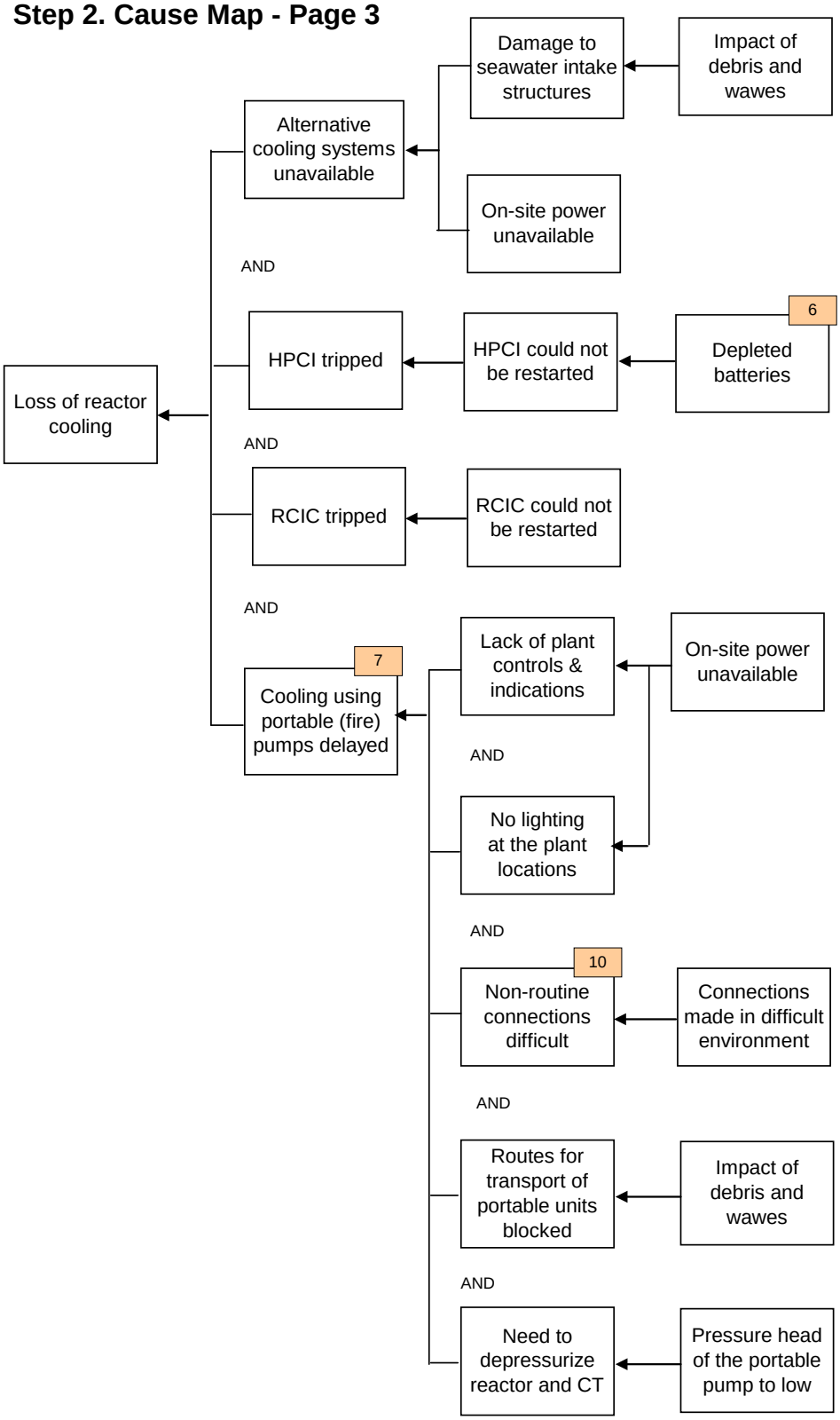
Severe core damage occurred because there was no cooling of the core for a long time. TEPCO estimates that following the loss of high pressure coolant injection (approximately 36 hours after reactor trip) there was no injection into the reactor for 6 hours and 43 minutes. This led to severe overheating and partial melt of the fuel. Residual heat was at a relatively high level as the Unit 3 was under operation at the onset of the event.

Step 2. Cause Map - Page 2



© ENCO

Step 2. Cause Map - Page 3



Hydrogen explosion in the reactor building was caused by the formation of explosive mixture of hydrogen and air in the reactor building. The lack of core cooling to compensate for decay heat resulted in excessive fuel temperatures and oxidation of the zirconium cladding. The oxidation of

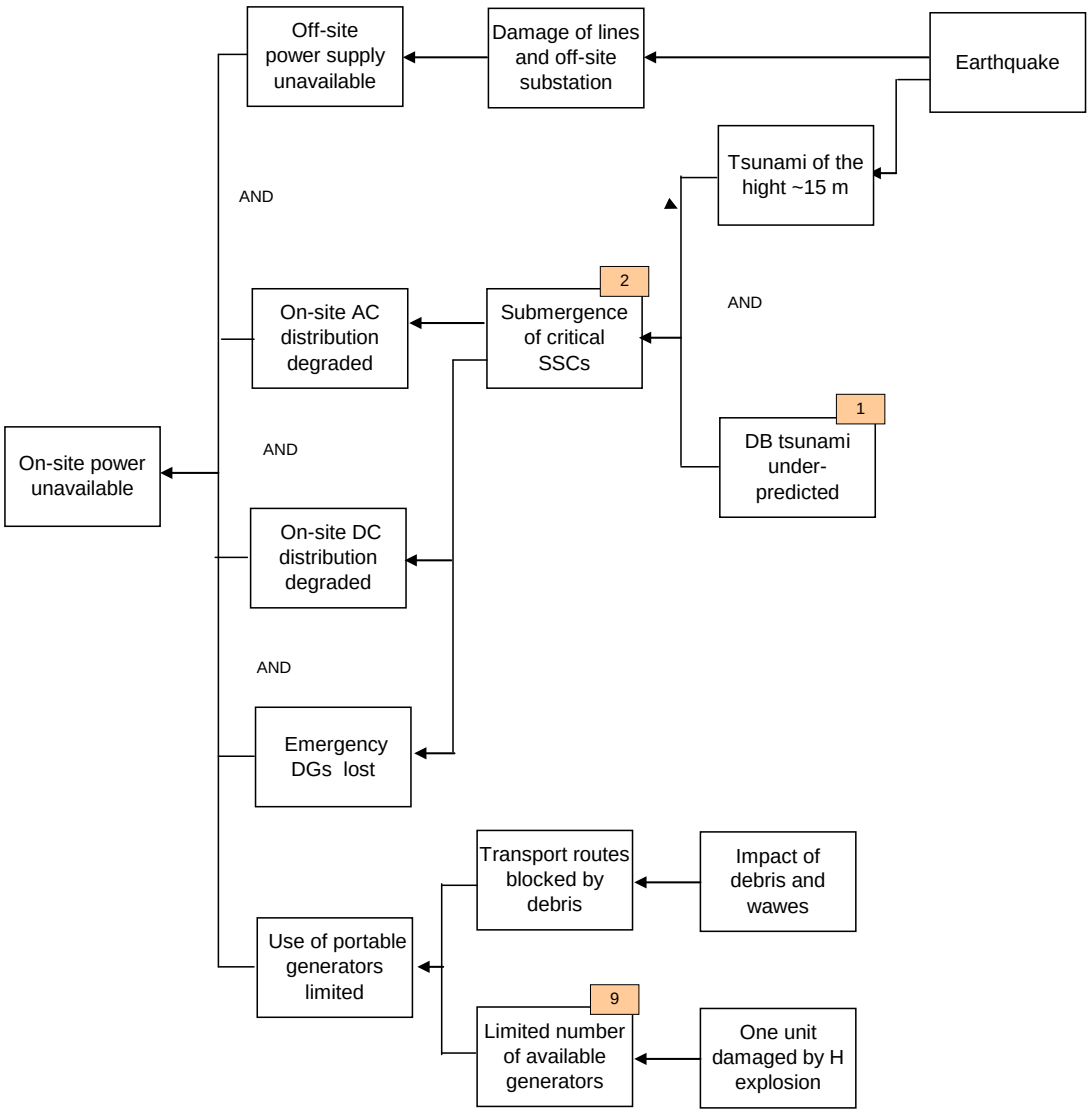
© ENCO

zirconium in a steam environment creates significant additional heat from the exothermic reaction and large quantities of hydrogen. This hydrogen contributed to the increases in containment pressure and to the subsequent hydrogen explosion. The extended duration of high temperature and pressure conditions inside containment may have damaged the drywell head seals, leading to hydrogen leaks and the subsequent explosions.

Venting of containment was delayed because of difficulties with providing power and compressed air for opening of vent valves (MOV and AOV). In addition, all work had to be conducted in a difficult working environment. The torus room was very hot because of the previous use of RCIC, HPCI, and SRVs and the room was completely dark. Increased radiation level also contributed to these difficulties.

Loss of reactor cooling was caused by the loss of high pressure emergency core cooling systems HPCI and RCIC. RCIC shut down unexpectedly and could not be restarted. HPCI tripped and could not be restarted due to depleted batteries. Other potential high pressure cooling systems (SLC, CRD) as well as low pressure systems (CS, RHR, RHRS) were non-functional due to loss of AC power as well as the loss of heat sink sources.

Step 2. Cause Map - Page 4



© ENCO

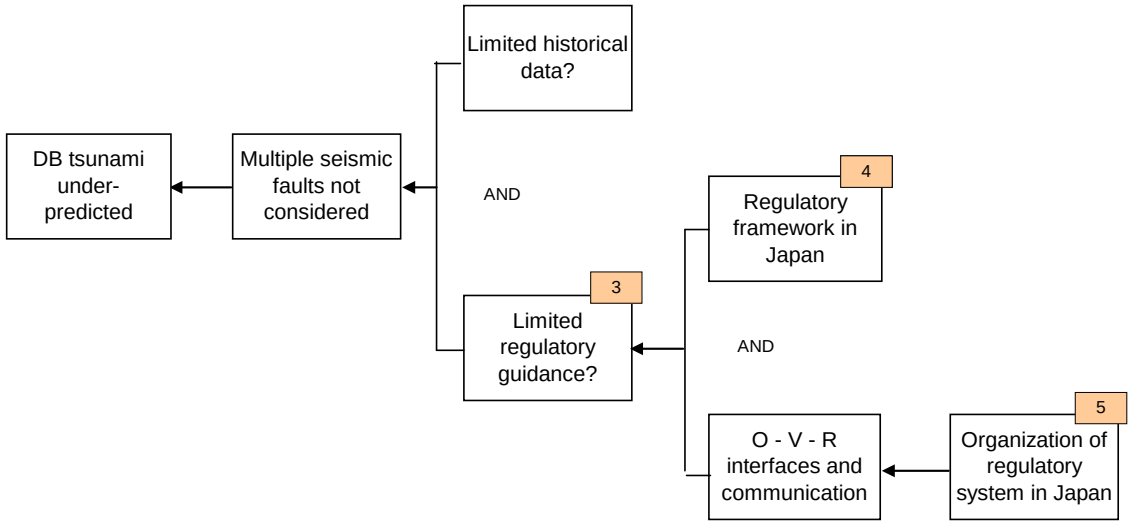
There were also problems with using portable fire engines. Out of the three fire engines Fukushima Daiichi had available, one was damaged by the tsunami and a second could not reach units 1-4 because of earthquake damage to the road. Only one fire engine was immediately available to support the emergency response on units 1-4.

Use of this fire engine required non-routine connections that had to be established in a difficult environment (increased temperature, radiation and in darkness). Additional problem, caused by the loss of on-site power, was the lack of indications and controls of valves involved in the implementation of the required lineup.

The fire engine did not have sufficient discharge pressure to overcome the elevation differences and reactor pressure. Personnel actions associated with depressurization of reactor and venting of the containment, necessary for reducing reactor pressure to the level acceptable for the use of fire engine, were not accomplished in time and failed to prevent core damage.

On-site power was lost because of the loss of off-site power and the loss of emergency diesel generators (EDGs). Off-site power was lost because of earthquake which damaged breakers and distribution towers. Following the earthquake, the on-site power relayed on EDGs which started on loss of offsite power. This source was lost because of tsunami. Tsunami resulted in flooding of both the EDGs and the on-site electrical distribution system (switchgear rooms). Submergence of critical SSCs in the power supply system resulted in the complete loss of AC power and led to a partial loss of DC power. All DC power was lost on units 1 and 2, while some DC power from batteries remained available on Unit 3.

Step 2. Cause Map - Page 5



Extensive damage of the electrical power supply system at the site was caused by the tsunami impacting the site that exceeded the design basis of the plant. The maximum tsunami height was estimated to be 14 to 15 meters as compared to the design basis tsunami height of 5.7 meters. This was above the site grade levels of 10 meters at units 1- 4. The seawater intake structure was also severely damaged and was rendered nonfunctional.

The tsunami protection strategy for the plant consisted of locating critical equipment, such as vital seawater pump motors, above the elevation of the assessed tsunami height. The assessment of the tsunami height was based on the 2002 Tsunami Assessment Method for Nuclear Power Plants in Japan, the accepted methodology by the Japanese industry. Following the guidance of this methodology, offshore fault segments were not combined in the tsunami assessment. During the

earthquake event numerous fault segments acted in combination, and thus the actual tsunami caused by the earthquake significantly exceeded the tsunami assessment for the plant.

Fundamentally, following the accepted tsunami assessment technical guidance in Japan resulted in under-prediction of the size of the tsunami. As a result, the plant tsunami protection strategy was not adequate and beyond-design-basis tsunami protection adequate to mitigate the effects of the tsunami that occurred was not available.

The issue of specifying appropriate tsunami design basis is not straightforward. This issue should be considered in the light of existing historical data consistently with the risk considerations. It seems that the regulatory framework that could be used by the nuclear industry in Japan for adequate protection of NPPs against tsunami was lacking clarity. Appropriate regulatory strategy and framework for protection of NPPs against natural hazards, which would appropriately balance defense-in-depth and risk considerations, was lacking. One of the reasons may be the structure of regulatory authority that is composed of several organizations. This issue requires further analysis.

Step 3. Analysis of solutions

The Cause Map is used to identify all the possible solutions for the problem so that the best solutions can be selected. Potential solutions correspond to those causes which can be controlled by the problem owner (Operator, Vendor, TSO organization, Regulator) so that the problem is prevented from recurring.

The following causes, which can be subject of interest in this context, can be identified on the Cause Map for the March 11 Fukushima tsunami accident (as developed in Step 2):

1. Design Basis tsunami under-predicted;
2. Submergence of critical SSCs due to flooding;
3. Limited regulatory guidance on the seismic and flooding protection of structures, systems, and components for operating plants;
4. Regulatory framework for adequate protection not adequate;
5. Organization of regulatory system in Japan complicated and unclear;
6. Depleted batteries/capabilities too low;
7. Cooling using portable pumps delayed;
8. Containment venting delayed;
9. Limited number of portable generators available at the site;
10. Non-routine connections of portable cooling pumps difficult to be accomplished in time.

These causes are related to various elements of the defence-in-depth protection of safety of nuclear power plants. The potential solutions are briefly discussed below.

Clarifying the Regulatory Framework

A logical, systematic, and coherent regulatory framework for adequate protection against external events that appropriately balances defence-in-depth and risk considerations should be established.

Such framework should clearly specify the requirements that allow the industry to determine the protections covered within the design basis and those to be considered as beyond-design-basis (i.e. part of the emergency preparedness plan). In particular, appropriate regulatory endorsed guidance should be available to specify the design basis tsunami. Such guidance should provide a clear basis for answering the question "What should be the design basis tsunami given the existing historical data and plant specific seismic information?"

Ensuring Protection

Given the design basis tsunami the licensees should ensure that the critical SSCs are adequately protected against seismically induced flooding.

Licensees need to re-evaluate and upgrade as necessary the design-basis seismic and flooding protection of structures, systems, and components for each operating plant. The regulator

should enforce appropriate corrective actions and ensure adequate oversight of their implementation.

Enhancing Mitigation

The licensees should strengthen station blackout mitigation capability at operating and new plant for design-basis and beyond-design-basis accidents induced by external events, including:

- Increasing the capability of batteries;
- Ensuring availability of portable generators and enhancement of their use during prolonged station blackout conditions;
- Enhancement of methods to reduce reactor pressure and feed cooling water to the reactor using portable cooling means /pumps;
- Ensuring additional sources of coolant water for the reactor;
- Enhancement of methods for non-routine connections of portable cooling means and ensure plant features to facilitate their realization during prolonged station blackout conditions;
- Enhancement of the containment venting system so that it is independent of AC power and operates with limited operator actions from the control room.

A.3. Bibliography for Annex A

"*Fukushima Daiichi Accident – Technical Causal Factor Analysis*", EPRI Report #°1024946, Final Report, March 2012.

"*Special Report on the Nuclear Accident at the Fukushima Daiichi Nuclear Power Station*", No. INPO 11-005, Revision 0, November 2011.

"*Regulatory Guide for Reviewing Seismic Design of Nuclear Power Reactor Facilities*", Nuclear Safety Commission (NSC, Japan), Document No. NSCRG: L-DS-I.02, September, 2006.

"*Tsunami Assessment Method for Nuclear Power Plants in Japan*", The Tsunami Evaluation Subcommittee, The Nuclear Civil Engineering Committee, Japan Society of Civil Engineers (JSCE), 2002 and 2006.

"*Report of the Japanese Government to the IAEA Ministerial Conference on Nuclear Safety - The Accident at TEPCO's Fukushima Nuclear Power Stations*", Nuclear Emergency Response Headquarters, Government of Japan, June, 2011.

"*International Conference on Advances in Nuclear Power Plants- Fukushima Accident: An Overview*", Akira Omoto, University of Tokyo, May 3, 2011.

"*Fukushima Nuclear Accident Analysis Report (Interim Report)*", Tokyo Electric Power Company, December 2011.

"Fukushima Analysis 11 03 2011 – In-depth Analysis of the Accident at Fukushima on 11 March 2011 With Special Consideration of Human and Organisational Factors", Swiss Federal Nuclear Safety Inspectorate (ENSI).

"*Recommendations for Enhancing Reactor Safety in the 21st Century*", The Near-Term Task Force Review of Insights from the Fukushima Dai-ichi Accident, U.S. Nuclear Regulatory Commission, July 12, 2011.

Epstein, W., "A PRA Practioner Looks at the Fukushima Daiichi Accident", Visiting Scholar, Ninokata Lab, presentation at Tokyo Institute of Technology, March 20, 2012.

8 Annex B. Overview of Air France 447 crash

B.1. Accident Summary

On 31 May 2009, flight AF447 took off from Rio de Janeiro Galeão airport bound for Paris Charles de Gaulle. The airplane was in contact with the Brazilian ATLANTICO ATC centre on the INTOL – SALPU – ORARO route at FL350.

At around 2 h 02, the Captain left the cockpit. At around 2 h 08, the crew made a course change of about ten degrees to the left, probably to avoid echoes detected by the weather radar.

At 2 h 10 min 05, following the obstruction of the Pitot probes in an ice crystal environment, the speed indications became erroneous and the automatic systems disconnected. In the ensuing confusion, the pilots lost control of the airplane because they reacted incorrectly to the loss of instrumentation and then seemed unable to comprehend the nature of the problems they had caused. The airplane's flight path was not brought under control by the two copilots, who were rejoined shortly after by the Captain. The disengagement of the autopilot, and the pilot making nose-up inputs despite stall warnings, caused a fatal loss of airspeed and a sharp descent. The airplane went into a stall that lasted until the impact with the sea at 2 h 14 min 28.

Additionally, investigation into the accident revealed that the pilots had not received specific training in "manual airplane handling of approach to stall and stall recovery at high altitude", and that this was not a standard training requirement at the time of the accident.

Bodies and some airplane parts were found from 6 June 2009 onwards by the French and Brazilian navies. The investigation into the accident was initially hampered by the lack of eyewitness testimony on the flight and radar tracks, as well as by the lack of main parts of the airplane and the absence of any data from the flight recorders, which were located and recovered from the ocean floor in May 2011, nearly two years after the accident.

B2. Causal analysis

Step 1 - Definition of the problem

What	Problem(s)	Plane crash
When	Date	1st June 2009
	Time	2 h 14 min 28 (UTC)
	Different, unusual, unique	Thunderstorm/cluster of powerful cumulonimbus
Where	State, city	Atlantic Ocean, near the TASIL point, 3°03′57″ N 30°33′42″ W
	Facility, site	Air France
	Unit, area, equipment	Airbus A330-203, Registered F-GZCP
	Task being performed	Passenger flight AF447 – Rio de Janeiro to Paris

Impact to the Goals

Safety	216 passengers and 12 crew members onboard died
Public Safety	n/a
Environmental	n/a
Customer Service	Eroded confidence in Air France safety
Property, Equip., Mtls	Loss of the aircraft, estimated cost $ 200.000.000
Labor, Time	Costly investigations of the crash site
Frequency	Very rare

© ENCO

As a direct result of the event 216 passengers and 12 crew members were killed in the aircraft crash. This is an impact to the safety goal. Loss of the aircraft worth of ~$200,000,000 contributes to the property loss goal.

The Airbus AF447 crash had also an impact on the customer service goal. The AF447 crash was subject of broad interest to the public and media, and may have a negative impact on the confidence in Air France safety. The goal related to labor is impacted because the investigations of the crash site were complicated, long lasting, required use of costly equipment and involved intensive labor.

Step 2 – Analysis of causes (Causal Map)

The Cause Map is started with the goal related to safety. Safety goal was impacted because 228 people were killed in the aircraft crash. Property goal is impacted because an expensive aircraft (estimated value of ~$200,000,000) was lost.

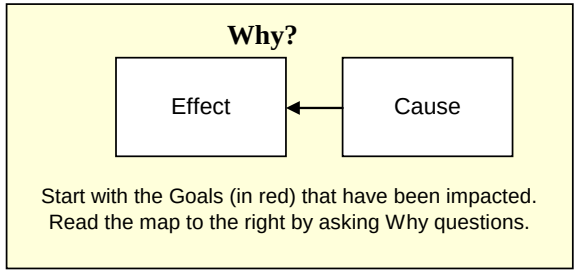
The plane broke to pieces due to impact with the sea. The plane was unable to maintain altitude due to loss of the lift. The plane lost the lift because AF447 pilots maintained a nose-up attitude that led to an aerodynamic stall. It resulted in losing altitude at 11,000 feet per minute. The plane fell for ~3 minutes 30 seconds and it hit the water nose up 16-degrees and belly first.

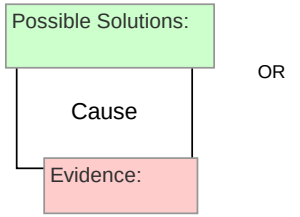
This situation happened because the flight control automation system disconnected and the pilots failed to control the plane manually. In normal flight conditions (so called "Normal Law") the Airbus has an electronic protective envelope (Automatic Pilot and Automatic Thrust) created by the set of flight control computers where the airplane can't over-bank, pitch up and stall, fly too slow or fly too fast. However, the "Normal Law" system was disconnected and plane control handed over to pilots (so called "Alternate Law") because the plane lost calculated airspeed indications (CAS). The airspeed indications were lost because the airspeed sensors – Pitot probes – were clogged by ice.

At high altitude and low temperatures, water sometimes doesn't freeze. Instead, it hovers, but as soon as something solid – like a pitot tube – flies through it, the water flash-freezes to form ice. Until heaters can melt the ice, the pitot probes are out. Without them, a plane's flight computer had no way to determine speed, and the automatic system shut down reverting plane to manual control.

Pitot probes problem was caused by the formation of ice inside the pitot tubes, because the plane passed into clouds associated with a large system of thunderstorms. Unlike other planes' crews flying through the region, AF447's flight crew has not changed the route to avoid the worst of the storms. The outside temperature was much warmer than forecast, preventing the still fuel-heavy aircraft from flying higher to avoid the effects of the weather. Instead, it ploughs into a layer of clouds.

The pitot probes on Airbus F-GZCP were produced by a French company, Thales, and the model was known as Thales AA. These Pitot probes were more vulnerable than most other models used currently. In the years leading up to the crash of Flight 447, the Thales AA model was problematic in places where the meteorological conditions like those at Tasil Point.

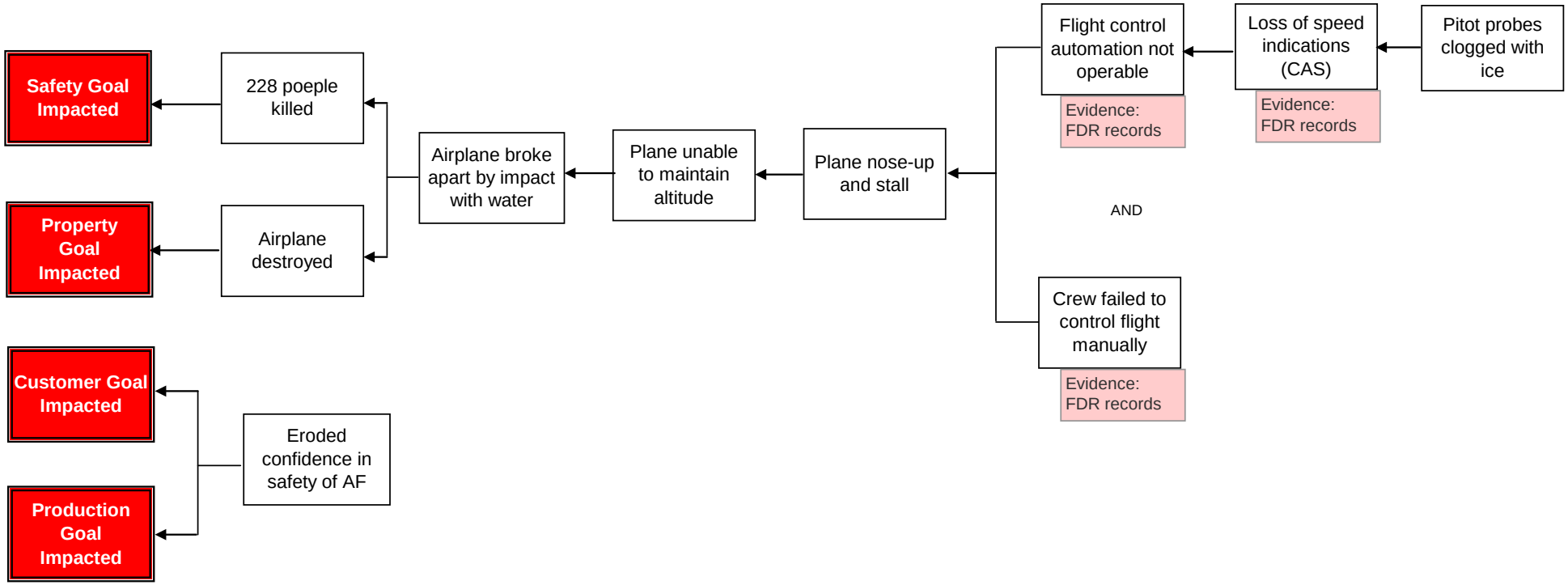




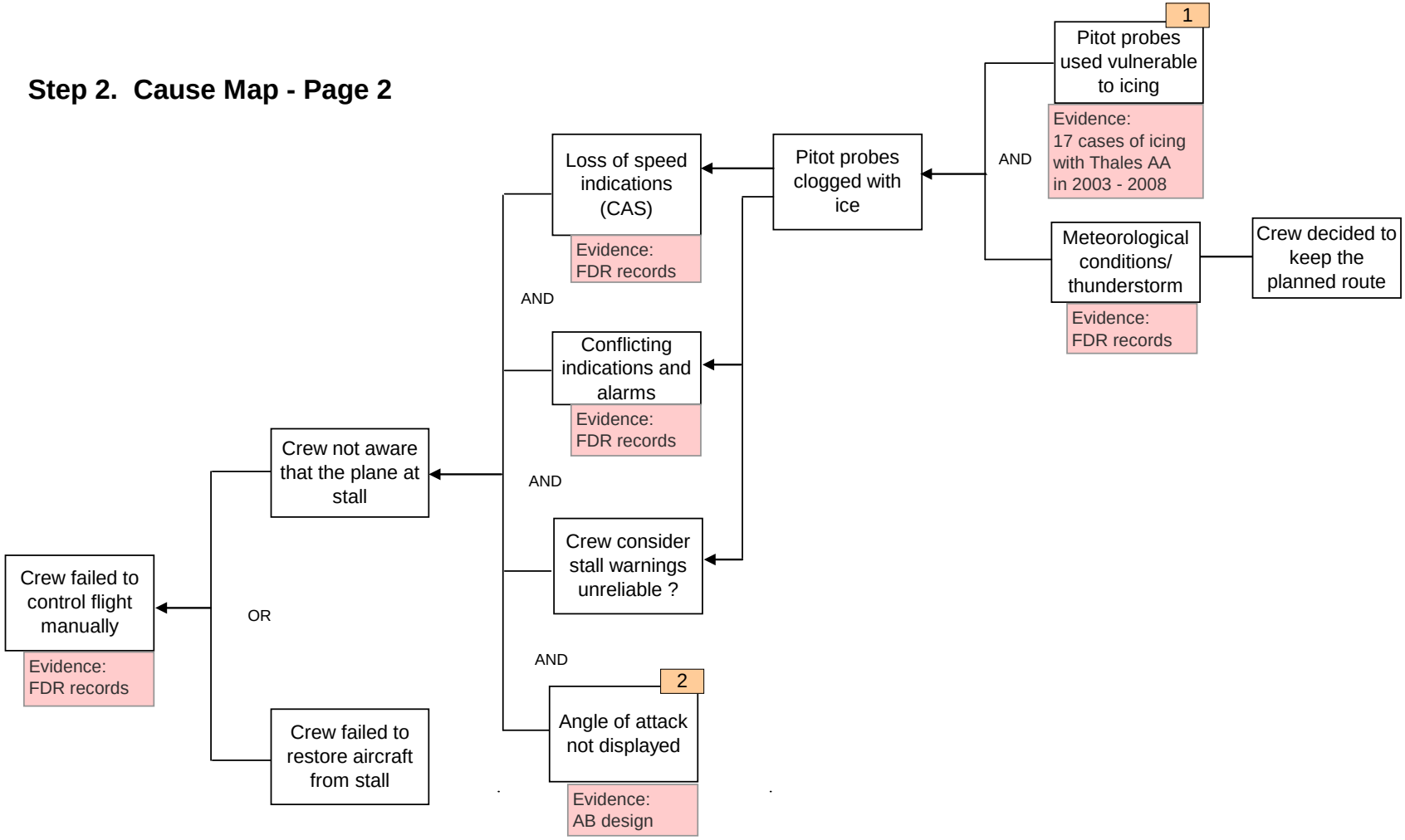
AND

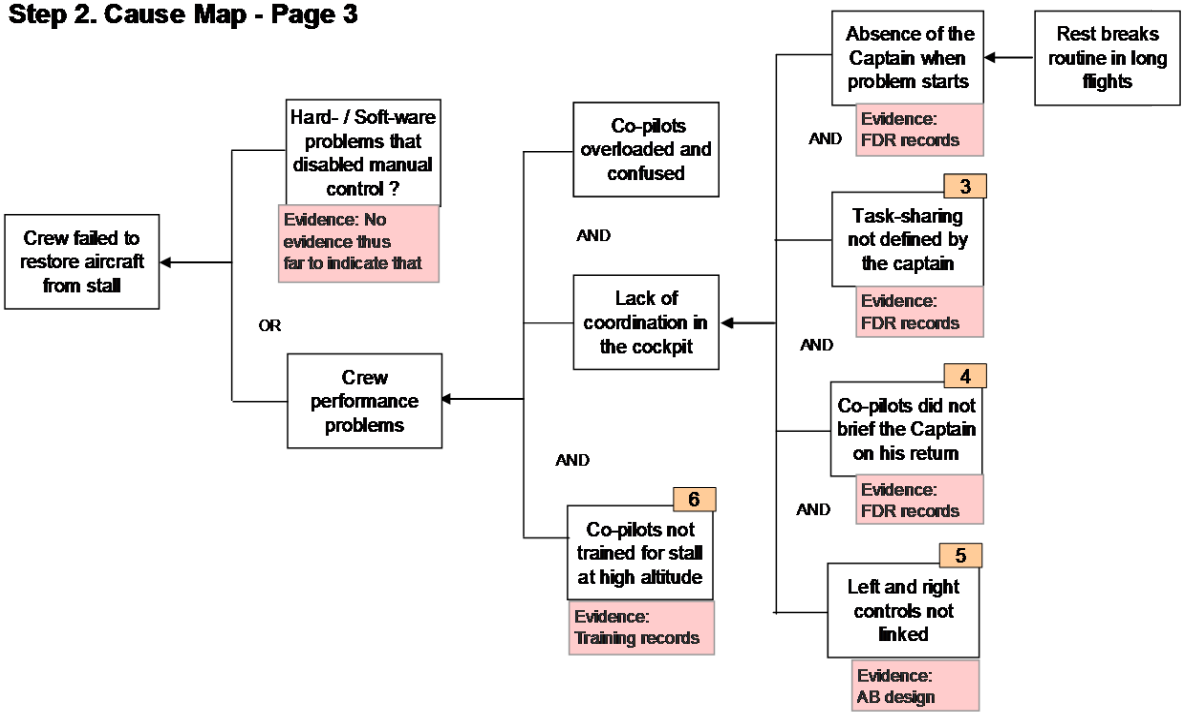
OR

Step 2. Cause Map - Page 1



Step 2. Cause Map - Page 2





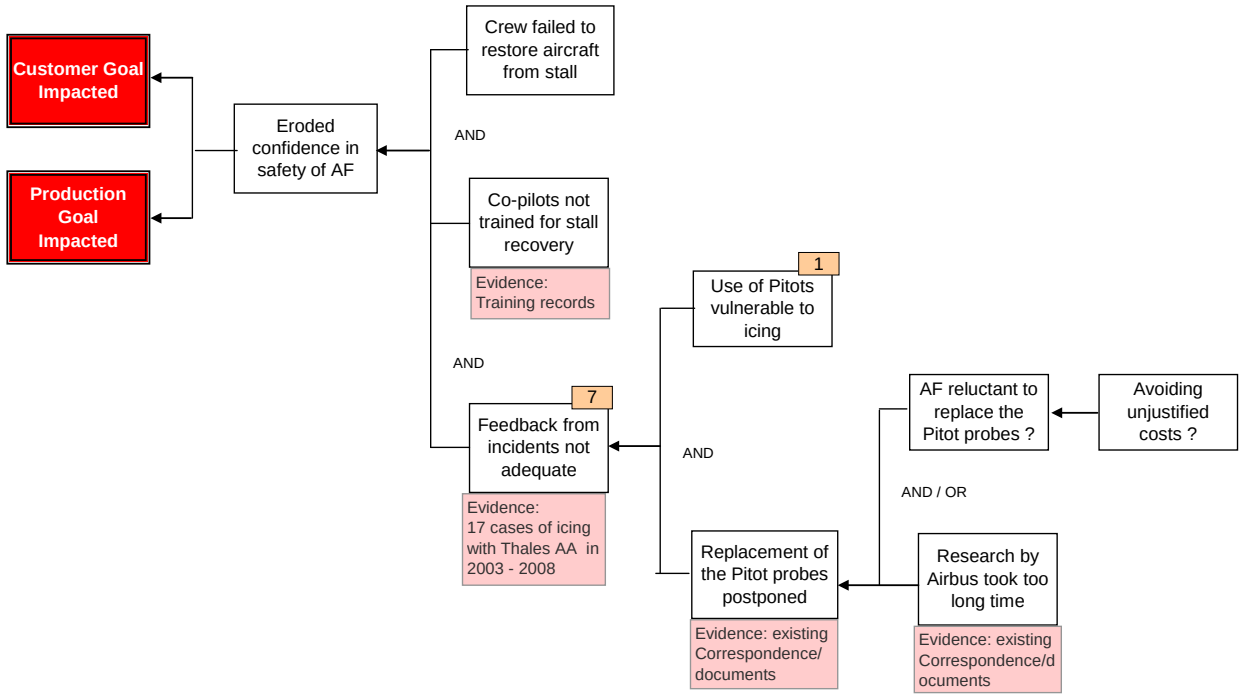
Important factor was also the lack of co-ordination in the cockpit. The interaction between the two co-pilots during the moments of crisis demonstrates remarkably poor communication, despite their training in crew resource management. Moreover, there was a marked lack of situational awareness, with everyone focusing on a few small details while ignoring a blaring cockpit alarm, which repeated the word “stall” 75 times before the plane crashed.

This co-ordination issue has even a broader nature. It started with the captain leaving the cockpit to take rest without explicitly clarifying who's in charge when two co-pilots are alone in the cockpit. They are failing, essentially, to cooperate. It is not clear to either one of them who is responsible for what, and who is doing what. In the opinion of Chris Nutter, an airline pilot and flight instructor, this is a natural result of having two co-pilots flying the plane. "When you have a captain and a first officer in the cockpit, it's clear who's in charge," Nutter explains. "The captain has command authority. He's legally responsible for the safety of the flight. When you put two first officers up front, it changes things. You don't have the sort of traditional discipline imposed on the flight deck when you have a captain."

The situation further worsens because the co-pilots did not brief the Captain on his return to the cockpit after his absence. None of the pilots mentions the stall warnings, or acknowledge the possibility that the plane has indeed stalled – even though the "Stall!" alarms were repeated in the cockpit many times. From his seat, the captain was unable to infer from the instrument displays in front of him why the plane is behaving as it is. The critical missing piece of information: the fact that someone has been holding the controls all the way back for virtually the entire time. No one has told the captain, and he hasn't thought to ask.

Another important aspect that contributed to the poor co-ordination within the cockpit is that left and right controls are not linked. The side sticks on an Airbus are "asynchronous" – that is, they move independently. "If the person in the right seat is pulling back on the joystick, the person in the left seat doesn't feel it," says Dr. David Esser, a professor of aeronautical science at Embry-Riddle Aeronautical University. "Their stick doesn't move just because the other one does, unlike the old-fashioned mechanical systems like used in small planes, where if you turn one, the [other] one turns the same way." PNF has no idea that, despite their conversation about descending, PF has continued to pull back on the side stick.

Step 2. Cause Map - Page 4



The potential negative impact on the confidence in Air France safety is associated with the high interest of the public and much speculation following the crash as well as opinions of aviation experts and aviators broadly expressed in the media and internet forums. It is worth noting that not all these opinions may be rationally justified, however, they may have impact on the confidence in safety of Air France as well as Airbus aircraft itself. It is worth noting that we haven't seen the unpleasant side of this yet. There will be a civil trial somewhere down the line and embarrassing questions will be asked.

Potential issues that may affect this confidence include: unsatisfactory performance of the crew, lack of adequate pilot's training provided by Air France, and inadequate feedback from past incidents. Two first issues have already been highlighted in the context of safety goal and property goal. The last one is discussed below.

Between 2003 and 2008, there were at least 17 cases in which the Thales AA had problems on the Airbus A330 and its sister plane, the A340. In September 2007, Airbus issued a “service bulletin” suggesting that airlines replace the AA pitots with a newer model, the BA, which was said to work better in ice.

In response, Air France’s official policy was to replace the AA pitots on its A330 planes “only when a failure occurred.” In August 2008, executives at Air France asked Airbus for proof that the BA pitots worked better in ice, and faced with the question, Airbus conceded that it did not have proof. So it removed the claim from the service bulletin. Another five months passed.

During that time, another airline, Air Caraïbes, experienced two incidents with the Thales AA on its Airbus A330s. The company’s chief executive immediately ordered the part removed from the fleet and alerted European regulators, who then began asking questions. In their conversations with Airbus, regulators learned of the 17 cases of icing, and they also discovered, looking at those cases, that the failures seemed to be happening more often (9 of the 17 occured in 2008). None of the failures seemed to indicate an immediate danger, so the Thales AA were not removed from service. Regulators simply asked Airbus to watch the problem and report back in a year.

It wasn’t until April 2009 that Airbus delivered test results to Air France showing that the BA really did work better in ice conditions. By then, 19 months had passed since the service bulletin

suggesting the same thing, but now Air France made the change. At the end of April, the airline ordered replacement of AA probes by BA model for its A330s, and on May 26, the first batch of BA probes arrived. Five days later, when Flight 447 took off in Rio, the probes were still in an Air France warehouse, and none of them had been installed. All three pitots on Flight 447 were the Thales AA.

It is evident that the process of learning from experience in this case was not adequate. Implementation of the corrective actions took too long. It is worth noting that two weakpoints of significant importance for the AF447 crash, i.e. relatively high likelihood of icing of the pitot probes (confirmed by the existing operational experience) and the inadequate training of the pilots in handling the aircraft with degraded automatic system at cruise altitude, have not been properly assessed in terms of the risk. If they had been properly addressed the associated risk would have been significantly reduced.

Replacement of the Thales AA pitot probes for better BA model took a long time because AF did not want to make a costly investment without sound justifications. Research related to this issue conducted by the vendor (Airbus) also contributed to this delay. The regulator was aware of this issue, but decided that the issue does not create "an immediate danger".

Icing of pitot probes could happen to any kind of pitot probe, but by the summer of 2009, the problem of icing on the Thales AA was known to be especially common. Between 2003 and 2008, there were at least 17 cases in which the Thales AA had problems on the Airbus A330 and its sister plane, the A340.

Crew failed to control the plane manually. There are two causes for this failure: the lack of correct diagnosis of the situation and/or inadequate performance of the crew.

The existing evidence indicates that the crew did not realize that the plane is at stall. None of the pilots mention the stall warnings, or acknowledge the possibility that the plane has indeed stalled—even though the word "Stall!" blares through the cockpit many times. The lack of correct diagnosis of the situation was caused by faulty airspeed readings, multiple fault alarms and flight control handed to the pilots in Alternate Law (which a pilot only experiences in the training simulator). It seems that the pilots were unsure what was happening and why. In the situation when the instruments provided conflicting information about what is going on, the crew could have doubts regarding the correctness of the stall alarm.

One of the potential causes of the wrong diagnosis was also the lack of direct indication of the angle of attack. A direct readout of the angle of attack could enable crews to promptly identify the aerodynamic situation of the airplane and take the actions that are required.

Failure of the crew to manually control the plane was caused by the crew performance problem. The existing evidence does not indicate any problems with the aircraft hardware or software that would disable the manual control of the aircraft. The center of the problem lied on the pilots' response to a deep stall at high altitude.

There were several causes that contributed to the crew performance problems. First of all the pilots were confused with the situation and overloaded with the tasks, trying to make sense of the conflicting indications and a long list of "faults" and alarms in the cockpit, and the aircraft buffeted by turbulence.

Another important cause is that the recovery of the aircraft from a stall at the cruise altitude was not subject to adequate training. When looking into pilots training scheme, it can be found that they are trained mainly to avoid stalling, not to recover from it. This is because simulators can't really reproduce airplane behaviour in such instances, and conducting training of this type on real planes is expensive and frightening.

Step 3 – Analysis of solutions

The Cause Map is used to identify all the possible solutions for the problem so that the best solutions can be selected. Potential solutions correspond to those causes which can be controlled by the problem owner (Operator, Vendor, Regulator) so that the problem is prevented from recurring.

The following causes, which can be subject of interest in this context, can be identified on the Cause Map for the June 1 AF447 accident (as developed in Step 2):

1. Pitot probes used in the aircraft F-GZCP vulnerable to icing
2. Angle of attack not displayed
3. Task-sharing not defined by the captain
4. Co-pilots did not brief the captain on his return
5. Left and right controls not linked
6. Co-pilots not trained for stall at high altitude
7. Feedback from incidents not adequate

The potential solutions are briefly discussed below.

Vulnerability of Pitot probes to icing (cause 1)

The pitot probes used in Airbus 330, which had been found to be vulnerable to icing, needs to be replaced by a newer model that has been proved to work better in ice conditions. This solution has already been implemented by AF.

Enhancement of the existing airspeed indication system would also be desirable by introducing a backup airspeed system based on diverse airspeed sensors. This solution would reduce the probability of common cause failures – a weakpoint of the existing system that use 3 redundant pitot probes.

Direct accessibility of information on the angle of attack (cause 2)

Information on angle of attack, which in the current Airbus design is not directly accessible to the pilots, would enable crews to identify the aerodynamic stall conditions. Introducing such information on the display seems to be a solution that can be implemented relatively easily.

It worth to be noted that the angle of attack in cruise is close to the stall warning trigger angle of attack in a law other than normal law. Under these conditions, manual handling can bring the airplane to high angles of attack such as those encountered during the AF447 event. It is essential in order to ensure flight safety to reduce the angle of attack when a stall is imminent. Only a direct readout of the angle of attack could enable crews to rapidly identify the aerodynamic situation of the airplane and take the actions that may be required. Consequently, the BEA recommends that EASA and the FAA evaluate the relevance of requiring the presence of an angle of attack indicator directly accessible to pilots on board airplanes.

Crew resource management issues (causes 3-5)

There are 3 causes on the Cause Map that are closely related with the crew resource management. They include:

- Task-sharing not defined by the captain (cause 3)
- Co-pilots did not brief the Captain on his return (cause 4)
- Left and right controls not linked (cause 5).

The investigation showed that an absence of training and practice for a crew consisting of two copilots does not guarantee a level of performance equivalent to a crew consisting of a captain and a copilot when faced with a degraded situation. The absence of a hierarchy and of effective task-sharing in the cockpit strongly contributed to the low level of synergy. The anxiety generated by the absence of the captain from the cockpit shows that the two copilots were not capable of resolving this emergency situation. This can be explained both by the absence of any appropriate training and a lack of decision-making practice on the part of the two copilots.

Causes 3 and 4 should be addressed with the improvement of cockpit procedures and enhancement of the pilots' training programmes. Enhancement should focus on clear definition of criteria for the role of relief captain and ensuring better task-sharing in case of relief crews. The final investigation report issued by BEA includes similar recommendations.

Cause 5 is also associated with the crew resource management. Delinking the left and right controls of AB-330 was a design feature that contributed to the critical sequence of events leading to the AF447 catastrophic outcome. In a plane with the right and left seat controls linked, the PNF would have been able to detect PF's mistaken decision to lift the plane's nose and correct it.

Training of pilots for stall at high altitude (cause 6)

The pilots training scheme implemented by AF is lacking a comprehensive training on avoiding stalling and recovery from the stall conditions at cruise altitude. High altitude stall training in the simulator has to be emphasized, along the other lessons required.

The pilots have to learn that recovery of aircraft from a stall takes time and requires a significant loss of the plane altitude before recovery is accomplished (trade altitude for airspeed). The important thing for the pilot is to reduce the pitch and keep the trust to "Full" (TOGA) until the plane recovers stable flight at a considerably lower altitude where aerodynamic performance is increased.

The BEA in the final report [B-3] provides specific recommendations regarding such training. EASA is recommended to review the content of check and training programmes and make mandatory, in particular, the setting up of specific and regular exercises dedicated to manual aircraft handling of approach to stall and stall recovery, in particular at high altitude.

Feedback from incidents (cause 7)

The investigations of AF447 crash showed that the experience feedback process in place at Air France needs improvement. Analysis of incidents and near-misses should be conducted with a more careful consideration of potential risk aspects. Decisions on the implementation of appropriate correction actions need to be risk informed. It is evident that the risk of an accident comparable to the AF447 crash (in the light of the existing operational experience) has been underestimated and appropriate actions that would prevent severe accident have not been implemented in time.

Operating evidence indicates that the likelihood of Pitot probes icing was relatively high. At the same time deficiencies of the training programme related to plane stalling conditions and stall recovery at cruise altitude makes the likelihood of the catastrophic outcome not negligible. If such evaluation had been conducted the appropriate correction actions would have been implemented in time to prevent the AF447's disaster. It is worth noting that other incidents involving faulty speed readings emerged just weeks after the Air France 447 crash.

B.3. Bibliography for Annex B

BEA, "Interim Report on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris", issued on 2 July 2009.

BEA, "2nd Interim Report on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris", issued on 30 November 2009.

BEA, "3rd Interim Report on the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro – Paris", issued on 29 July 2011.

WISE, J., *"What Really Happened Aboard Air France 447"*, *Popular Mechanics,* December 6, 2011. http://www.popularmechanics.com/technology/aviation/crashes/what-really-happened-aboard-air-france-447-6611877

HYLTON, W. S., *"What Happened to Air France Flight 447?"*, New York Times, May 4, 2011; http://nyti.ms/air-france-447

PETERSON, B.,"*Blame the Pilots of Air France 447? Not So Fast*" http://www.popularmechanics.com/technology/aviation/crashes/are-the-pilots-of-air-france-447-to-blame-5818769?src=soc_twtr

Marks, P., "*Report on Air France 447 crash deepens mystery*", New Scientist blog, 27 May 2011. http://www.newscientist.com/blogs/onepercent/2011/05/blaring-alarms-confused-doomed.html

9 Annex C. Overview of Deepwater Horizon oil rig explosion

C.1. Accident Summary

On April 20, 2010 at approximately 9:45 pm a huge explosion rocked a semi-submersible Mobile Offshore Drilling Unit (MODU) located about 66 km off the coast of Louisiana in the Gulf of Mexico. The oil rig was called the *Deepwater Horizon* and was owned by Transocean Ltd and leased to the British Petroleum Company through September 2013.

The direct cause of the explosion was that high pressure methane gas from the well expanded into the drilling riser and was released onto the drilling rig, where it ignited and exploded, engulfing the rig.

At the time of the explosion, there were 126 crew on board: 7 employees of BP, 79 of Transocean, as well as employees of various other companies involved in the operation of the rig, including Anadarko, Halliburton and M-I Swaco. Most of the workers escaped the rig by lifeboat and were subsequently evacuated by boat or airlifted by helicopter for medical treatment. However, eleven workers were never found despite a three-day Coast Guard search operation, and are believed to have died in the explosion. 16 workers were injured.

Efforts by multiple ships to douse the flames were unsuccessful. After burning for approximately 36 hours, the Deepwater Horizon sank on the morning of 22 April 2010.

Remotely operated submersible vehicles were used to examine the wellhead. The vehicles were also used in an effort to manually trigger the blowout preventer (BOP), which would close the wellhead and prevent any farther release of oil. The blowout preventer is a 450-ton valve installed at the wellhead that is designed to automatically shut to prevent oil leaks in the event of an accident. Attempts to manually close the blowout preventer have not been successful.

An oil leak was discovered on the afternoon of 22 April when a large oil slick began to spread at the former rig site. Oil continued to leak from the wellhead more than a mile underwater on the ocean floor at an estimated rate of 42,000 gallons a day. According to the Flow Rate Technical Group, the leak amounted to about 4.9 million barrels (780,000 m^3) of oil, exceeding the 1989 Exxon Valdez oil spill as the largest ever to originate in U.S.-controlled waters.

C.2. Causal analysis

Step 1 - Definition of the problem

What	Problem(s)	*Deepwater Horizon* oil rig explosion and oil spill
When	Date	April 20, 2010
	Time	21:49
	Different, unusual, unique	Deepwater drilling
Where	State, city	Gulf of Mexico, Louisiana, United States 28°44′12.01″ N 88°23′13.78″ W
	Facility, site	Macondo well
	Unit, area, equipment	*Deepwater Horizon* oil rig platform
	Task being performed	Process of temporary abandoning the well

Impact to the Goals

Safety	11 fatalities, 16 injured
Public Safety	Extensive damage to marine and wildlife habitats and to the Gulf's fishing and tourism

Environmental	Significant release of oil, offshore pollution
Customer Service	Drilling operation in the area suspended
Property, Equip., Mtls	Complete loss of the rig (appr. cost $700 mln)
Labor, Time	Massive efforts to terminate the oil spill
Frequency	Very rare

Step 2 – Analysis of causes (Causal Map)

Property goal was impacted because the oil rig was burned up and sunk. Safety goal was impacted because of the explosion and fire led to 11 fatalities and 16 persons injured. Environmental goal was impacted because the explosion and fire led to significant release of oil to the environment. Production goal was impacted because the drilling operations in the region were suspended for several months. Labor goal was impacted because the release of oil required significant efforts to terminate the spill.

The oil rig was burned up and sunk because of the loss of well control and hydrocarbons blowout. Hydrocarbons were released onto the rig because the well integrity was not established during the temporary abandonment process.

There were two physical barriers that have been designed to seal the well – the annulus cement barrier and cement plug in the shoe track. Both of these barriers failed to contain hydrocarbons within the geologic formation (reservoir).

Influx of hydrocarbons from the formation to the well through the imperfect cement barriers was induced by the end-of-well activities – displacing the mud from the riser and replacing it with seawater. This made the well underbalanced because the mud is much heavier than seawater.

Rig crew failed to disconnect the well using the blank shear ram (BSR) because the crew did not recognize gas influx in time. BOP emergency disconnect system also failed to terminate blowout. Flammable gases penetrated the engine area and ignited causing explosion and severe fire.

Integrity of annulus cement barrier

Annulus cement barrier (see Cause Map - Page 2, Cause A) was ineffective in sealing the well because of three potential causes: (i) deficiencies of cement slurry design, (ii) deficiencies of cementing job, and (iii) problems with placing cement in the well.

Cement slurry design was critical because of the pore pressure and fracture gradient – however the technical review of the slurry design gave heavy emphasis to preventing lost returns. If cementing procedure placed too much pressure on the geologic formation below, it might trigger another lost-returns event similar to the one on April 9. In this case, critical cement – not mud – might flow into the formation and be lost, potentially leaving the annular space at the bottom of the well open to hydrocarbon flow.

BP chose to use “nitrogen foam cement” – a cement formula that has been leavened with tiny bubbles of nitrogen gas, injected into the cement slurry just before it goes down the well. This formula was chosen to lighten the resulting slurry from approximately 16.7 pounds per gallon (ppg) to 14.5 ppg – thereby reducing the pressure the cement would exert on the fragile formation. The bubbles, in theory, would also help to balance the pore pressure in the formation and clear the annular space of mud as the cement flowed upward.

Lab tests carried out as part of the investigation suggest that the slurry was unstable at drilling depth pressures and temperatures and there was likely to be nitrogen breakout. The slurry was not fully tested before use.

There were several cement slurry design features that could have led to foam instability and contributed to a failure of the cement barrier. These include: the extremely low cement slurry yield point, additive of a defoamer, and lack of fluid loss control additives.

Potential instability factors were also the possibility of cement slurry contamination because of no bottoms up circulation, relatively low rate of pumping cement, and small volume of cement.

BP's plan was to limit the circulation of drilling mud through the wellbore before cementing. Optimally, mud in the wellbore would have been circulated "bottoms-up" – meaning the rig crew would have pumped enough mud down the wellbore to bring mud originally at the bottom of the well all the way back up to the rig. Such extensive circulation cleans the wellbore and reduces the likelihood of channelling (see Section 2.3 for additional explanations). And circulating bottoms-up allows technicians on the rig to examine mud from the bottom of the well for hydrocarbon content before cementing.

But the BP engineers feared that the longer the rig crew circulated mud through the casing before cementing, the greater the risk of another lost-returns event. Accordingly, BP circulated approximately 350 barrels of mud before cementing, rather than the 2,760 barrels needed to do a full bottoms-up circulation.

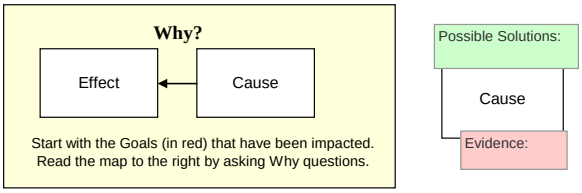
BP decided to pump cement down the well at the relatively low rate of 4 barrels or less per minute. Higher flow rates tend to increase the efficiency with which cement displaces mud from the annular space. But the increased pump pressure required moving the cement quickly would mean more pressure on the formation (ECD) and an increased risk of lost returns. BP decided to reduce the risk of lost returns in exchange for a less-than-optimal rate of cement flow.

BP made another compromise by limiting the volume of cement that would be pumped down the well. Pumping more cement is a standard industry practice to insure against uncertain cementing conditions: more cement means less risk of contamination and less risk that the cement job will be compromised by slight errors in placement. But more cement at Macondo would mean a higher cement column in the annulus, which in turn would exert more pressure on the fragile formation below.

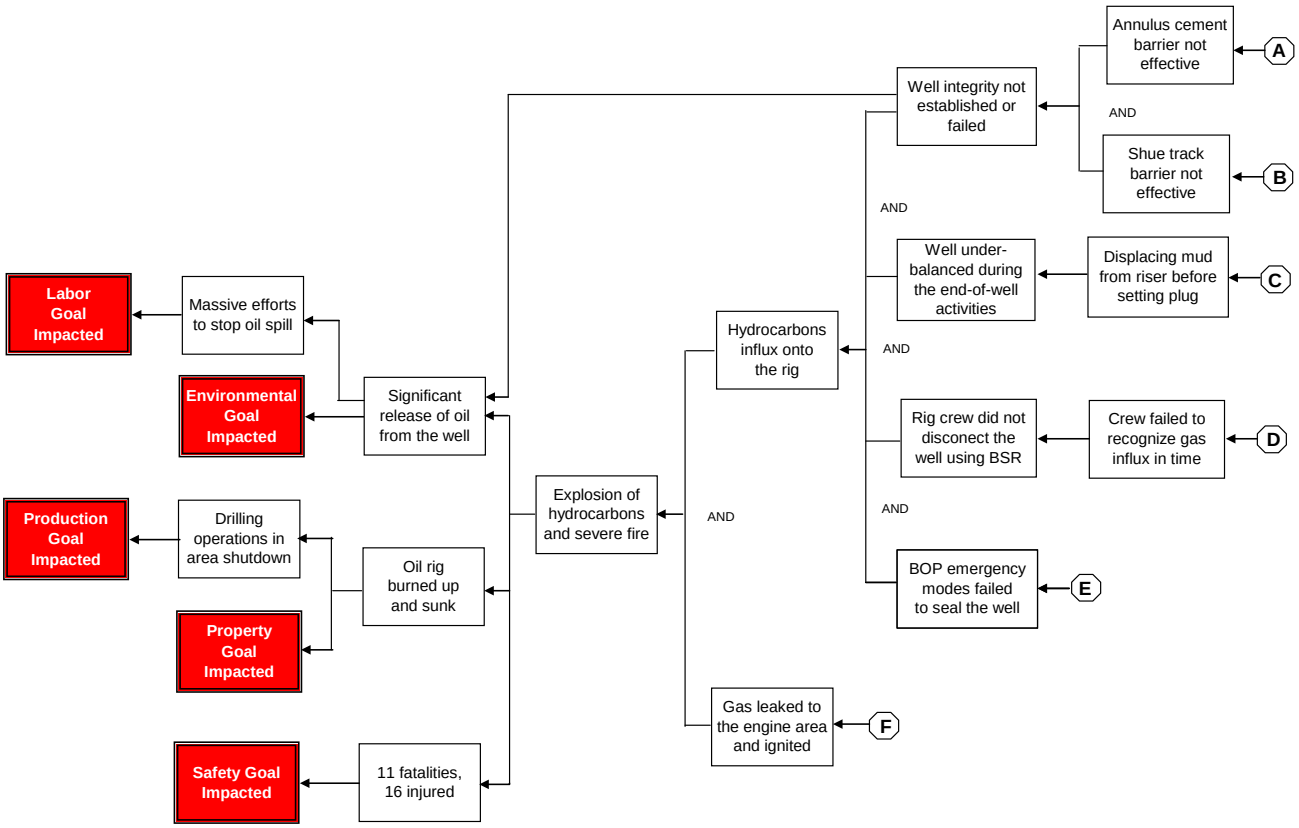
Accordingly, BP determined that the annular cement column should extend only 500 feet above the uppermost hydrocarbon-bearing zone (and 800 feet above the main hydrocarbon zones), and that this would be sufficient to fulfill MMS regulations of "*500 feet above the uppermost hydrocarbon-bearing zone*". However, it did not satisfy BP's own internal guidelines, which specify that the top of the annular cement should be 1,000 feet above the uppermost hydrocarbon zone.

The integrity of cement barriers was also affected by the design of the cement job. There were two important factors that increased potential for channeling: the use of long string casing and a limited number of centralizers.

The 18,300 ft long 400-ton casing string had a 5,800 ft long lower portion with 7-inch diameter. Most of the hole over this portion of casing was 9.875-inch diameter. However, the lowest 180 ft of 7-inch casing with 4 equi-spaced centralizers was squeezed into an 8.5-inch hole with only 56 ft of rathole bottom clearance. Compressed sediment and granular infill in the 0.75-inch wide annulus (Halliburton's best practices document recommends 1.5 to 2-inch annular gap tolerance) most probably explains the need for much-higher-than-normal pressure of 3142 psi to liquefy it (at the ninth attempt) and allow mud to circulate. The unexpected high pressure and subsequent lower-than-specified mud flow led to problems with conversion of float collar (as discussed in the context of the integrity of shoe track barrier).



Step 2. Cause Map - Page 1

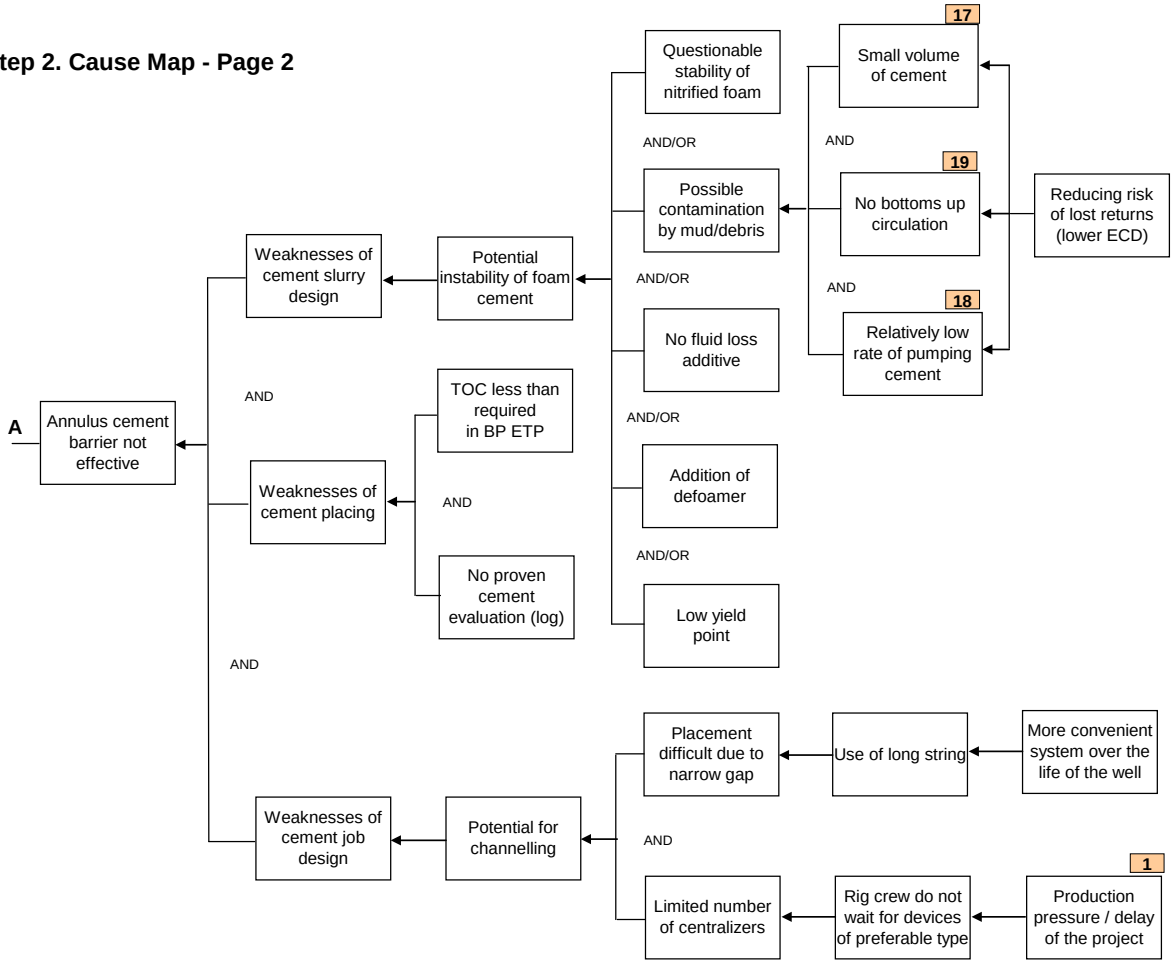


Centralizers are critical components in ensuring a good cement job. The evidence to date does not unequivocally establish whether the failure to use 15 additional centralizers was a direct cause of the blowout. But the process by which BP arrived at the decision to use only six centralizers at Macondo illuminates the flaws in BP's management and design procedures, as well as poor communication between BP and Halliburton.

It does not appear that BP's team tried to determine before April 15 whether additional centralizers would be needed. Had BP examined the issue earlier, it might have been able to secure additional centralizers of the design it favored. Nor does it appear that BP based its decision on a full examination of all potential risks involved. Instead, the decision appears to have been driven by an aversion to one particular risk: that slip-on centralizers would hang up on other equipment.

BP did not inform Halliburton of the number of centralizers it eventually used, let alone request new modeling to predict the impact of using only six centralizers. Halliburton happened to find out that BP had run only six centralizers when one of its cement engineers overheard a discussion on the rig.

Step 2. Cause Map - Page 2



It needs to be noted that the decisions on the use of long casing string, limited number of centralizers, and Top Of Cement (TOC) lower than in BP's Engineering Technical Practice, which had potential impact on the integrity of cement annular barrier, were convenient from the production point of view or intended to save time and money.

The BP team erred by focusing on full returns as the sole criterion for deciding whether to run a cement evaluation log. The BP Macondo team used final lift pressure and returns to confirm successful cement placement and decided no further evaluation was needed. However, this was not in line with procedures which state that more rigorous evaluation is required in some circumstances.

Cement evaluation logs plainly have their limitations, particularly at Macondo. But while many companies do not run cement evaluation logs until the completion phase, BP should have run one here – or sought other equivalent indications of cement quality in light of the many issues surrounding and leading up to the cement job.

Integrity of shoe track barrier

Potential causes that led to a failure of the shoe track barrier (see Cause Map – Page 3, cause B) include two items: inadequate quality of shoe track cement and failure of flapper valves to seal.

Inadequate quality of shoe track cement barrier could have been caused by the contamination of shoe track cement due to nitrogen breakout (from the foam cement used for the annular space), contamination of shoe track cement by mud in the wellbore, inadequate design of shoe track cement (tail cement), and swapping of the shoe track cement by mud in the rathole (bottom of the well).

Contamination of the shoe track cement by mud was more likely because of the oil-based spacer used by the crew. While drilling crews routinely use water-based spacer fluids to separate oil-based

drilling mud from seawater, the spacer BP chose to use during the negative pressure test was a mixture of two different lost-circulation materials left over on the rig – the heavy, viscous drilling fluids used to patch fractures in the formation when the crew experiences lost returns.

BP wanted to use these materials as spacer in order to avoid having to dispose of them onshore as hazardous waste[1]. Material of this type had never previously been used by anyone on the rig or by BP as a spacer, nor been thoroughly tested for that purpose.

Two flapper valves, which create additional element of the shoe track barrier, could have failed because of three possible mechanisms: failure to convert the flow collar, damage due to high load needed to establish circulation (see Section 2.3 for discussion of pressure anomalies during the preparation of the well for cementing job), and random failure of the two flapper valves.

Whether the float valves converted contributing to the blowout, has not yet been, and may never be, established with certainty. But, what is certain is that BP's team failed to take time to consider whether and to what extent the anomalous pressure readings may have indicated other problems or increased the risk of the upcoming cement job.

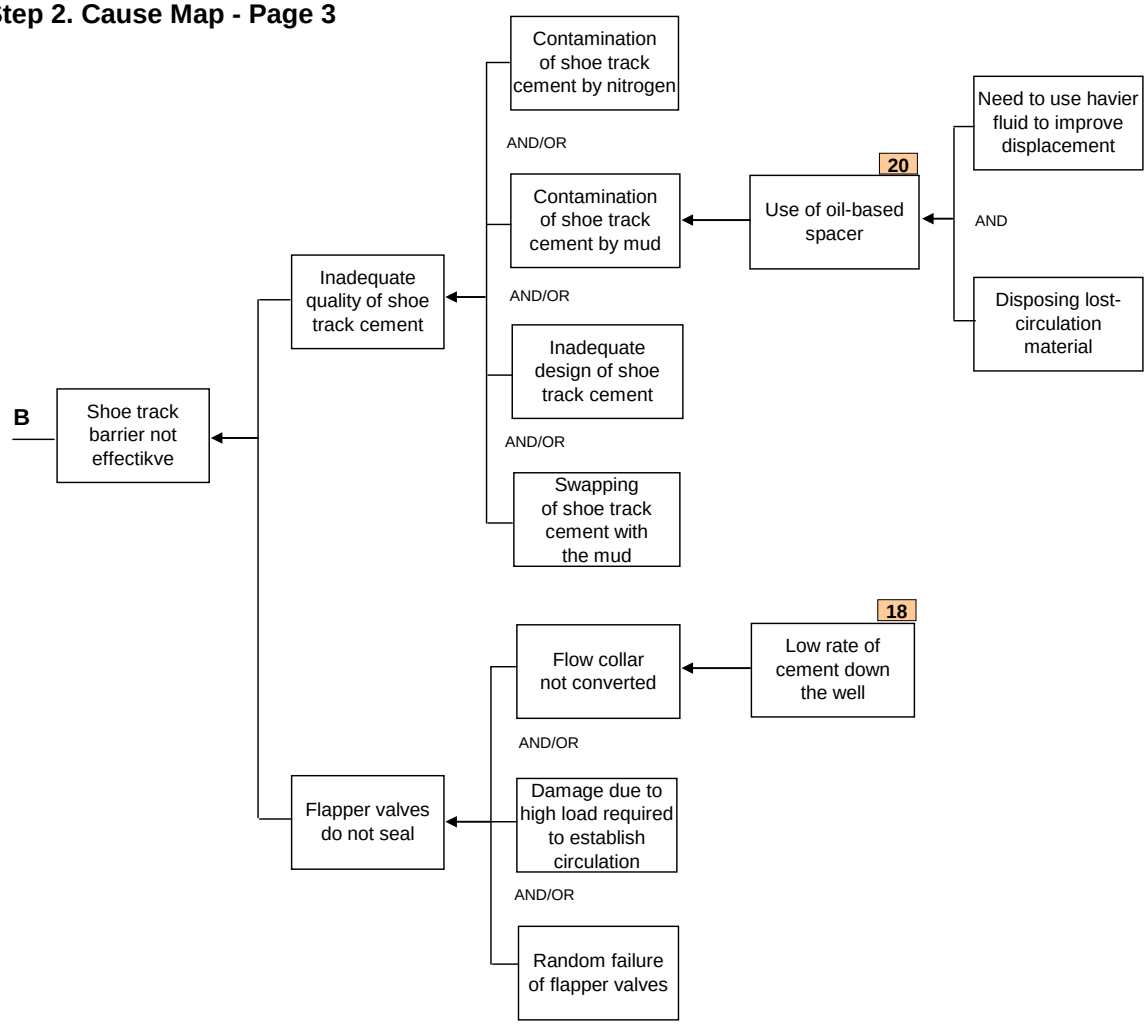
BP's team appears not to have seriously examined why it had to apply over four times the 750 psi design pressure to convert the float valves. More importantly, the team assumed that the sharp drop from 3,142 psi meant the float valves had in fact converted. That was not at all certain. The auto-fill tube was designed to convert in response to flow-induced pressure. Without the required rate of flow, an increase in static pressure, no matter how great, would not dislodge the tube.

While BP's Macondo team focused on the peak pressure reading of 3,142 psi and the fact that circulation was reestablished, it does not appear the team ever considered whether sufficient mud flow rate had been achieved to convert the float valves. They should have considered this issue. Because of ECD concerns, BP's engineers had specified a very low circulating pump rate – lower than the flow rate necessary to convert the float valves. BP does not appear to have accounted for this fact.

High load applied to establish circulation could have damage the flapper valves and resulted in their failure to prevent blowout. It is also possible that the failure of flapper valves to seal was a random failure, although likelihood of coincident failures of two valves seems to be low.

[1] Pursuant to the Resource and Conservation Recovery Act, exploiting an exception that allows companies to dump waterbased "drilling fluids" overboard if they have been circulated down through a well

Step 2. Cause Map - Page 3



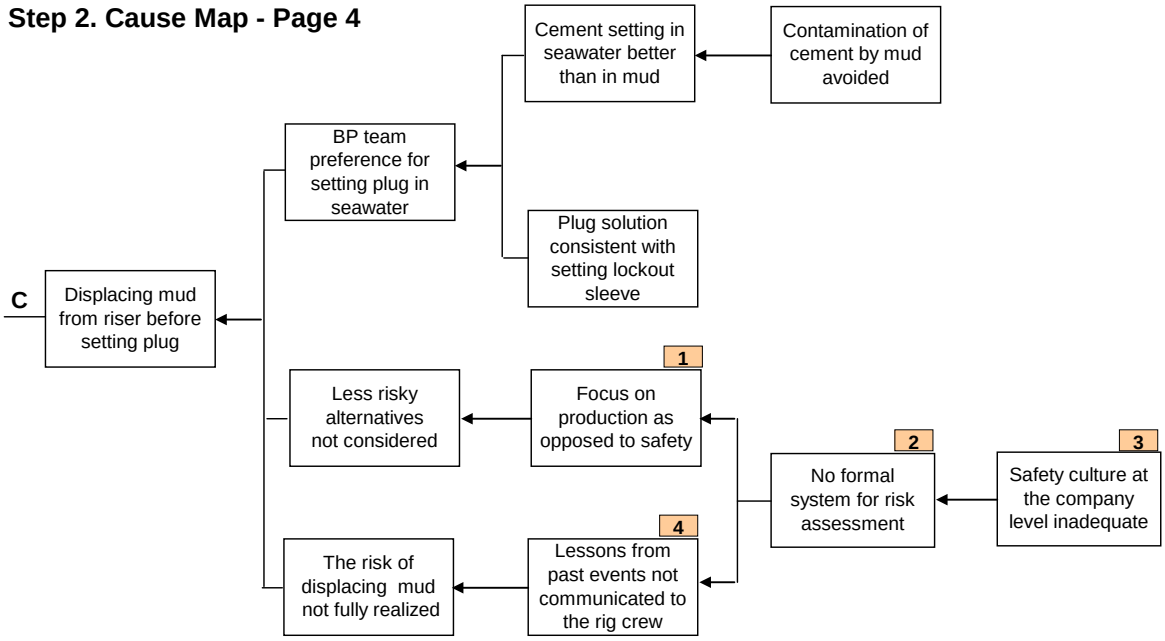
Displacement of mud from the riser

Decision regarding displacement of mud from the riser before setting cement plug (see Cause Map – Page 4, Cause C) was an important factor that have contributed to the blowout. First, it was not necessary or advisable for BP to replace 3,300 feet of mud below the mud line with seawater. By replacing that much heavy drilling mud with much lighter seawater, BP placed more stress on the cement job at the bottom of the well than necessary. BP's stated reason for doing so was its preference for setting cement plugs in seawater rather than mud.

While industry experts have acknowledged that setting cement plugs in seawater can avoid mud contamination and that it is not unusual for operators to set cement plugs in seawater, BP has provided no evidence that it or another operator has ever set a surface cement plug so deep in seawater (particularly without additional barriers). The risks BP created by its decision to displace 3,300 feet of mud with seawater outweighed its concerns about cement setting better in seawater than in mud.

As BP has admitted, cement plugs can be set in mud. BP also could have set one or more non-cement bridge plugs (which work equally well in mud or seawater). No evidence has yet been produced that the BP team ever formally evaluated these options or the relative risks created by removing 3,300 feet of mud.

Step 2. Cause Map - Page 4



It is noted that setting the cement plug 3,300 feet below the mud line was not necessary. The BP Macondo team chose to do so in order to set the lockdown sleeve last in the temporary abandonment sequence to minimize the chances of damage to the sleeve. Setting the lockdown sleeve would require 100,000 pounds of force. The BP Macondo team sought to generate that force by hanging 3,000 feet of drill pipe below the sleeve – hence the desire to set the cement plug 3,000 feet below the mud line.

BP's desire to set the lockdown sleeve last did not justify the risks its decision created. BP could have used other proven means to protect the lockdown sleeve if set earlier in the process. It also did not need 3,000 feet of space to generate 100,000 pounds of force. There were some recommendations of BP experts for setting the plug roughly 1,300 feet below the mud line (using heavier drill pipe), rather than 3,300 feet down. That would have significantly increased the margin of safety for the well.

The most troubling aspect of BP's temporary abandonment procedure was BP's decision to displace mud from the riser before setting the surface cement plug or other barrier in the production casing. During displacement of the riser, the BOP would be open, leaving the cement at the bottom of the well (in the annulus and shoe track) as the only physical barrier to flow up the production casing between the pay zone and the rig. Relying so heavily on primary cement integrity put a significant emphasis on the negative-pressure test and well monitoring during displacement, both of which are subject to human error.

BP's decision under these circumstances to displace mud from the riser before setting another barrier unnecessarily and substantially increased the risk of a blowout. BP could have set the surface cement plug, or a mechanical plug, before displacing the riser. BP could have replaced the mud in the wellbore with heavier mud sufficient to overbalance the well. It is not apparent why BP chose not to do any of these things.

Decision making processes at Macondo did not adequately ensure that personnel fully considered the risks created by time- and money-saving decisions. Whether purposeful or not, many of the decisions that BP, Halliburton, and Transocean made that increased the risk of the Macondo blowout clearly saved those companies significant time (and money).

It is noted in Ref. [C-4] that choosing a less-costly or less-time-consuming alternative – as long as it is proven to be equally safe – is normal in commercial business. The problem is that, at least in regard to BP's Macondo team, there appears to have been no formal system for ensuring that alternative procedures were in fact equally safe. None of BP's (or the other companies') decisions

appear to have been subject to a comprehensive and systematic risk-analysis, peer-review, or management of change process.

Transocean failed to adequately communicate lessons from an earlier near-miss to its crew. Transocean failed to adequately communicate to its crew lessons learned from a similar near-miss on one of its rigs in the North Sea four months prior to the Macondo blowout. The basic facts of both incidents are the same. Had the rig crew been adequately informed of the prior event and trained on its lessons, events at Macondo may have developed very differently.

The above mentioned deficiencies indicate significant weaknesses in safety culture not only within BP, but also within other corporations involved in the Macondo project.

Kick detection

Failure of the rig crew to recognize influx of hydrocarbons into the well (see Cause Map – Page 5, Cause D) was an important factor that have contributed to the Macondo accident.

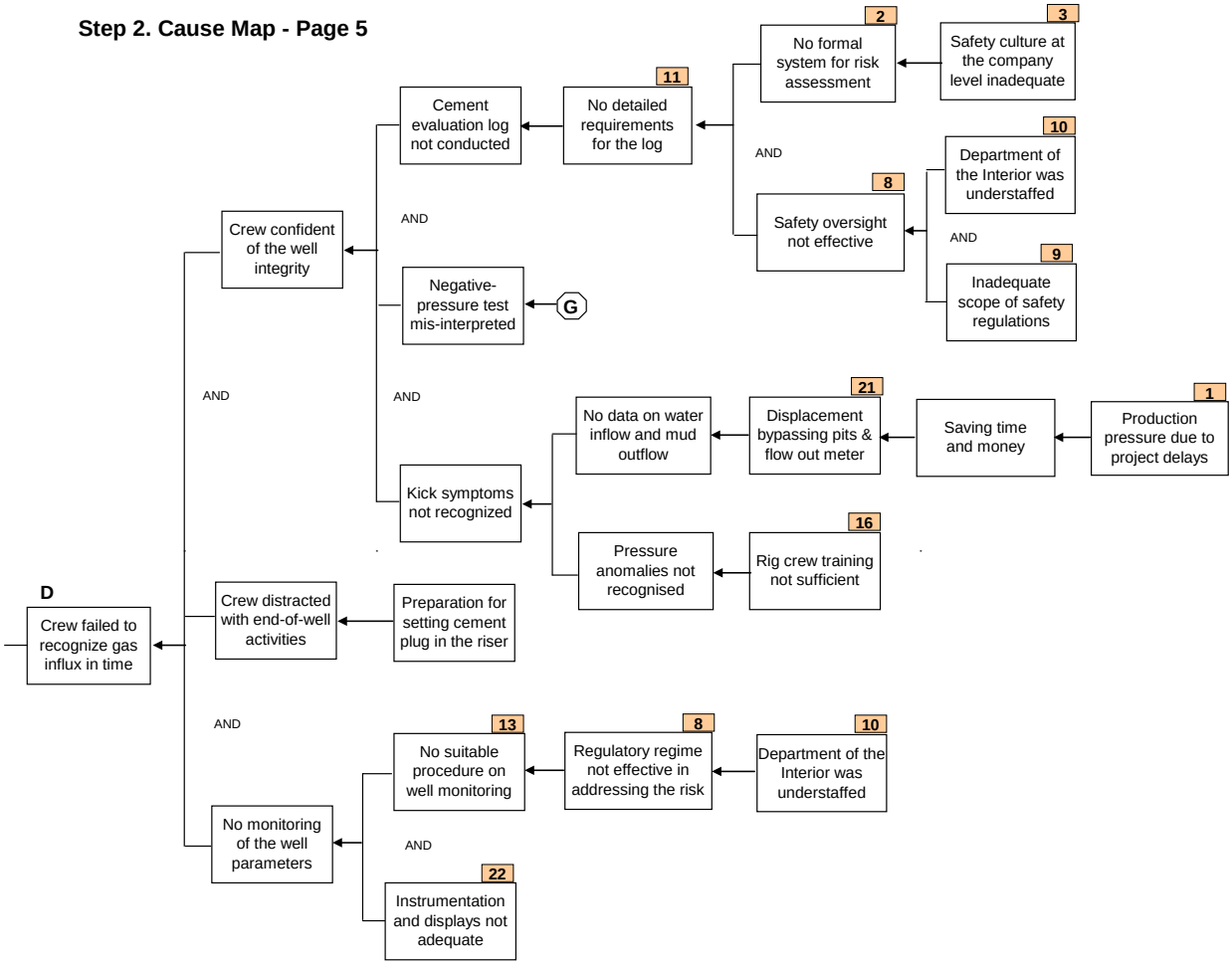
The crew could have prevented the blowout – or at least significantly reduced its impact – if they had reacted in a timely and appropriate manner. What is not now clear is precisely why the drilling crew and other individuals on the rig missed several critical signs indicating that a kick was occurring. There are several potential causes that can explain such behaviour.

The rig crew was confident regarding the integrity of the existing cement barriers. There was no systematic monitoring of the important parameters of the well that could help in detecting occurrence of a kick. Important factor was also that at the same time the crew was engaged in several end-of-well activities that could have distracted their attention.

The crew was confident that the existing cement barriers are effective based on the negative pressure test, results of which were misinterpreted. The cement evaluation log that could have identified potential barrier integrity problems was not conducted. The crew did not recognised anomalies in the well parameters that could have provided an indication of a kick.

Cement evaluation log was not conducted because the BP team was considering full returns as the sole criterion for deciding whether to run the evaluation log. Receiving full returns was a good indication that cement or other fluids had not been lost to the weakened formation. But full returns provided, at best, limited or no information about (i) the precise location where the cement had ended up, (ii) whether channelling had occurred; (iii) whether the cement had been contaminated; or (iv) whether the foam cement had remained stable. Although other indicators – such as on-time arrival of the cement plugs and observation of expected lift pressure – were reassuring, they too provided limited information. Other cement evaluation tools could have provided more direct information about cementing success.

BP team decision of not conducting a cement evaluation log did not fully conform to the intent of its own guidelines ETP GP 10-60. These guidelines require that top of cement (TOC) barrier should be 1000 ft above any distinct permeable zone and centralization should extend to 100 ft above such zone.



If these conditions are not met, as in this case, TOC should be determined by a "*proven cement evaluation log*", which would be done during the completion phase of the well. There is no evidence of a documented risk assessment regarding annulus barriers. It is not clear what is the regulator's position regarding this issue.

There are several potential factors that may have contributed to the failure to properly conduct and interpret the negative pressure test that night.

There was no standard procedure for running or interpreting the test in either MMS regulations or written industry protocols. The regulations and standards did not require BP to run a negative-pressure test at all. BP and Transocean had no internal procedures for running or interpreting negative-pressure tests and had not formally trained their personnel in how to do so.

The crew engaged in conducting and interpreting the test were not fully aware of the associated risk. There were several factors that could have impact on the crew's appreciation of the risk.

Although many BP and Halliburton employees were aware of the difficulty of the primary cement job those issues were for the most part not communicated to the rig crew that conducted the negative-pressure test and monitored the well. It appears that BP did not even communicate many of those issues to its own personnel on the rig. BP well site leaders did not consult anyone on shore about the anomalous data observed during the negative-pressure test. Had they done so, the Macondo blowout may not have happened.

Due to poor communication, it does not appear that the staff performing and interpreting the test had a full appreciation of the context in which they were performing it. Such an appreciation might have increased their willingness to believe the well was flowing.

The rig crew missed several signs of a "kick" – that is, hydrocarbons in the riser -- on the night of a blowout. The Sperry Sun data available to the crew from between 8:00 p.m. and 9:49 p.m. reveal a number of different signals that if observed, should at least have prompted the driller to investigate further, for instance, by conducting a visual flow check, and then shutting in the well if there were indications of flow.

For instance, the increasing drill-pipe pressure after the pumps were shut down for the sheen test at 9:08 p.m. was a clear signal that something was happening in the well. Similarly, at roughly 9:30 p.m., the driller and toolpusher recognized an anomalous pressure difference between the drill pipe and kill line. Both of these signals should have prompted action – especially the latter: it was clearly recognized by the crew and coherent with the odd pressure readings observed during the negative-pressure test. The crew should have done a flow check and shut in the well, immediately upon confirmation of flow.

The crew missed or misinterpreted these signals. One possible reason is that they had done a number of things that confounded their ability to interpret signals from the well. For instance, after 9:08 p.m., the crew began sending fluids returning from the well overboard, bypassing the active pit system and the flow-out meter. Only the mudlogger performed a visual flow check. At 9:27 pm, less than 15 minutes before the blowout began, they did notice an anomaly in pressure data from the well, and shut down operations to investigate. They noticed several anomalies that should have caused serious concern, but showed no hint of alarm.

Another factor that prevented correct diagnosis of the problem was the lack of information regarding the flow parameters. Bypassing the active system and flow-out meter resulted in the lack of flow-in and flow-out data that could have indicated the well integrity problem. Had the crew routed the seawater through the active pit system before sending it into the well, such data would have been available.

Once the crew began displacing the riser with seawater, they confronted the challenge of dealing with all of the returning mud. The driller repeatedly rerouted the mud returns from one pit to another in order to accommodate the incoming volume. During that time, the crew also sent mud from other locations into the active pit system. It is not clear whether the crew could adequately monitor active pit volume (or flow-in versus flow-out) during that time given all the activity.

Important factor was also the lack of a suitable information system that would be capable to alert the crew when anomalies arise. In light of the potential consequences, the system used at the rig, which requires the right person to be looking at the right data at the right time, and then to understand their significance, in spite of simultaneous activities and other monitoring responsibilities, is not adequate.

The above mentioned deficiencies and missteps were rooted in systemic failures by industry management (extending beyond BP to contractors that serve many in the industry), and also by failures of government to provide effective regulatory oversight of offshore drilling. These are important root causes that must be properly addressed to prevent recurrence of similar accidents.

Failure of BOP emergency mode

Blowout preventer (BOP) was the last line of defence in the case of failure of the remaining barriers. The BOP is designed to contain pressure within the wellbore and halt an uncontrolled flow of hydrocarbons to the rig. The Deepwater Horizon's BOP did not succeed in containing the Macondo well.

Witness accounts indicate that the rig crew activated one of the annular preventers around 9:41 p.m., and pressure readings suggest they activated a variable bore ram (which closes around the drill pipe) around 9:46 p.m. Flow rates at this point may have been too high for either the annular preventer or a variable bore ram to seal the well. Earlier kick detection would have improved the odds of success.

After the first explosion, crew members on the bridge attempted to engage the rig's emergency disconnect system (EDS). The EDS should have closed the blind shear ram, severed the drill pipe, sealed the well, and disconnected the rig from the BOP. But none of that happened. When the subsea supervisor pushed the EDS button the panel indicators lit up, but the rig never disconnected.

Three potential causes can be identified for this failure. They include: failure of the control signal that activate the blind shear ram (BSR), failure of the hydraulic system that operate the shears, and BSR failure to slice through the drill pipe.

It is possible that the first explosion had already damaged the cables to the BOP, preventing the disconnect sequence from starting. Even so, the BOP's automatic mode function (so called "deadman" system) should have triggered the blind shear ram after the power, communication, and hydraulics connections between the rig and the BOP were cut. But the "deadman" system failed too.

Another possible cause is unavailability of two redundant control "pods" that control the BOP's automatic mode function (the "deadman" system). The deadman is designed to close the shear ram if the electronic and hydraulic lines connecting the rig to the blowout preventer are severed.

Post-incident testing of the two redundant "pods" revealed low battery charges in one pod and defective solenoid valves in the other. If those problems existed at the time of the blowout, they would have prevented the deadman system from working. This failure may have been due to poor maintenance.

Failure of the BSR hydraulic system is a potential single failure that could disable the BSR function. The likely cause is hydraulic fluid leak that may have reduced the ram cutting force. Failure of this system would have also prevented activation of BSR through the use of underwater robot (VOR).

Attempt to use VOR was undertaken within the first few days after the explosion. Using a robotic submersible equipped with a hydraulic pump, the crew injected seawater into the blind shear ram, hoping to drive its pistons and blades closed. But the pump did not have nearly the needed strength; it could not pump water at a sufficient rate to budge the blades.

It is also possible that BSR was not capable to shear the pipe. Two potential causes can be indicated: BSR blades are positioned on indestructible joint or the BSR cutting force is not sufficient to cut pipe.

The first possibility, for the BOP with only one BSR, as used by the Deepwater Horizon, is estimated as 0.10. The possibility of the latter scenario is confirmed by two studies of West Engineering Services of Brookshire, Tex., one of the industry's premier authorities on blowout preventers. These studies found a more basic problem: even when everything worked right, some blind shear rams still failed to cut pipe. West's experts concluded that calculations used by makers of blowout preventers overestimated the cutting ability of blind shear rams. It is noted that modern drill pipe is nearly twice as strong as older pipes of the same size. In addition, the intense pressure and frigid temperatures of deep water make it tougher to shear a pipe.

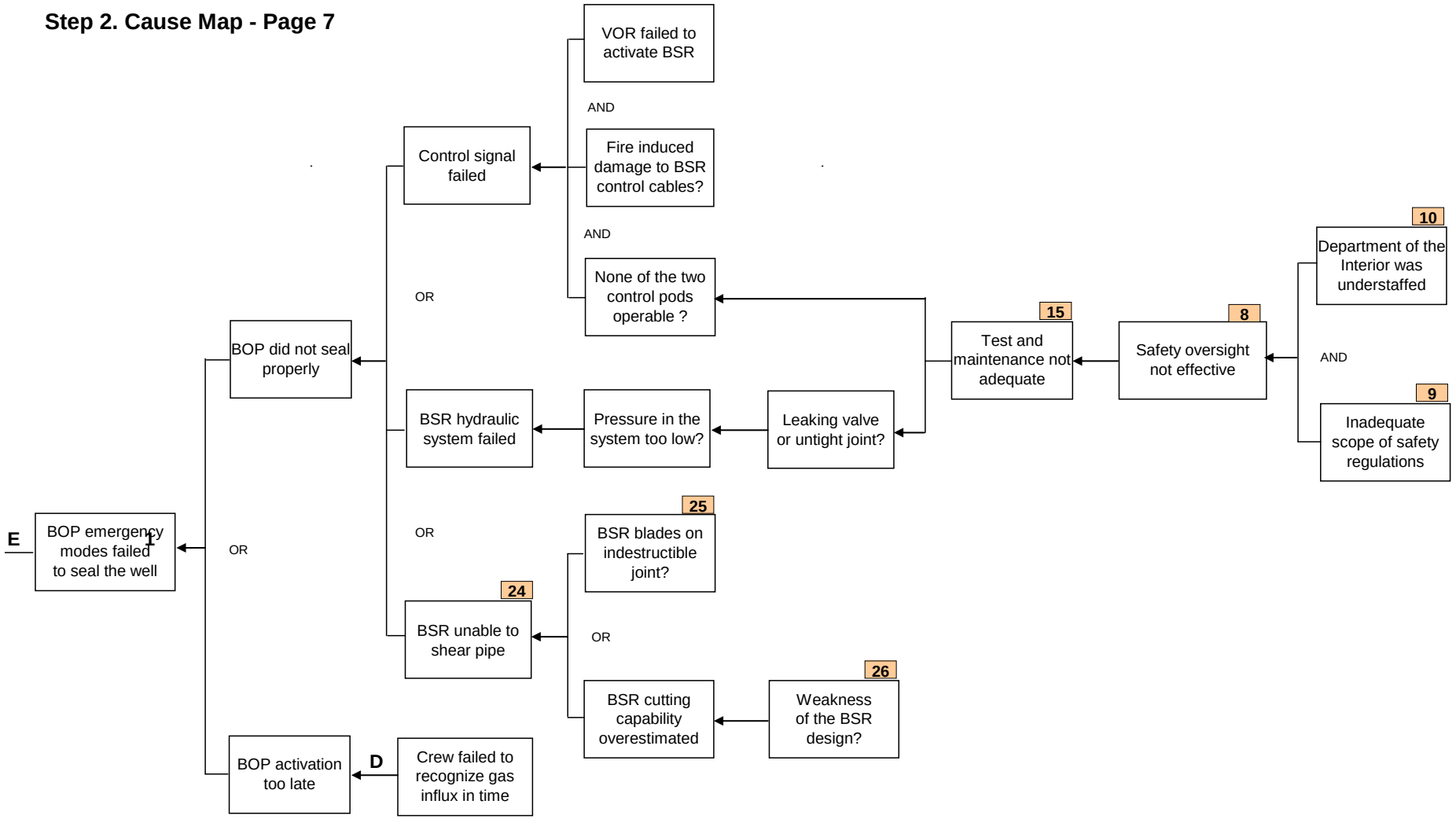
It is worth noting that from the point of view of reliability, BOP is rather a vulnerable device. In 2009 Transocean commissioned a "strictly confidential" study of the reliability of blowout preventers used by deepwater rigs. Using the world's most authoritative database of oil rig accidents, a Norwegian company, Det Norske Veritas, focused on some 15,000 wells drilled off North America and in the North Sea from 1980 to 2006. It found 11 cases where crews on deepwater rigs had lost control of their wells and then activated blowout preventers to prevent a spill. In only six of those cases were the wells brought under control, leading the researchers to conclude that in actual practice, blowout preventers used by deepwater rigs had a "failure" rate of 45 percent. The study also revealed that the BOP is vulnerable to a single failure of a control valve in the hydraulic system.

Diversion of flow to the MGS

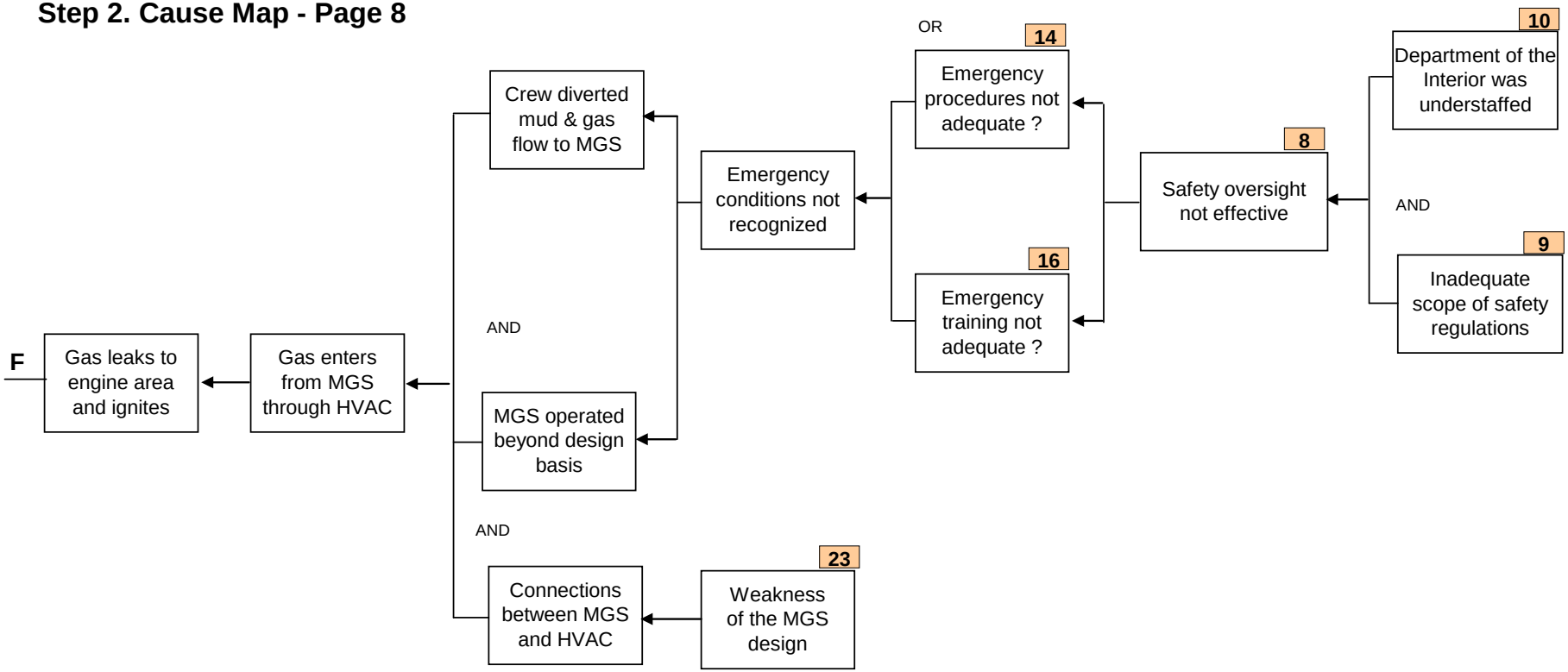
Direct cause of the ignition and explosion of blowout gases was that gas penetrated the engine area that was outside the fire protection area and had electrical equipment containing potential ignition sources. Gas entered the engine area from the mud gas separator (MGS) system through the rig's heating, ventilation and air conditioning system (HVAC).

When hydrocarbons flow was finally noted, the Deepwater Horizon crew closed the blowout preventer and diverter, routing oil and gas to the mud gas separator (MGS) system rather than diverting it overboard. The MGS was operated beyond design basis and was overwhelmed by the force of oil and gas which leaked into the rig's ventilation system. Gas was exiting the vents located on the derrick, directly above the rig floor.

Step 2. Cause Map - Page 7



Step 2. Cause Map - Page 8



It is not clear why personnel did not choose to divert the gas directly overboard. While that ultimately may not have prevented an explosion, diverting overboard would have reduced the risk of ignition of the rising gas. Considering the circumstances, the crew also should have activated the blind shear ram to close in the well. Diverting the flow overboard and/or activating the blind shear ram may not have prevented the explosion, but likely could have given the crew more time and perhaps limited the impact of the explosion.

There are a few possible explanations for why the crew responded in this way. The crew may not have recognized the severity of the situation, though that seems unlikely given the amount of mud that spewed from the rig floor. They did not have much time to act. The explosion occurred roughly six to eight minutes after mud first emerged onto the rig floor.

Perhaps the most significant factor is the lack of appropriate emergency procedure and training. The rig crew had not been trained adequately how to respond to such an emergency situation, including the simulations and drills for such emergencies, and momentous decision to engage the blind shear rams or trigger the EDS.

The heating, ventilation and air conditioning system is thought to have sent a gas-rich mixture into the engine rooms. Connections between MGS and HVAC indicate weaknesses of the design.

Step 3 – Analysis of solutions

The Cause Map is used to identify all the possible solutions for the problem so that the best solutions can be selected. Potential solutions correspond to those causes which can be controlled by the problem owner so that the problem is prevented from recurring.

The following causes, which can be subject of interest in this context, can be identified on the Cause Map for the Deepwater Horizon accident (as developed in Step 2):

General issues related to safety management, safety culture, and regulatory oversight

1. Focus on production as opposed to safety / production pressure
2. No formal system for risk assessment of alternative solutions
3. Safety culture at the company level inadequate
4. Lessons from potential issues or past events not communicated to the rig crew
5. Subcontractors failed to communicate adequately
6. Making *ad hoc* changes during well development without evaluation of the related risk
7. Well site management not consulting potential issues/anomalies with on shore office
8. Safety oversight of exploration, drilling and production of oil from deepwater formations not effective
9. Inadequate scope of safety regulations for deepwater oil industry
10. Department of the Interior responsible for safety oversight of deepwater oil industry understaffed.

Procedures and training

11. No detailed requirements for the cement log test
12. Standard BP procedure for negative-pressure test not detailed enough
13. No suitable procedure on well monitoring
14. Emergency procedures not adequate
15. BOP test and maintenance not adequate
16. Rig crew training not sufficient.

Process safety

17. Small volume of cement used in the well cementing process
18. Relatively low rate of pumping cement
19. No bottoms up circulation
20. Use of oil-based spacer
21. Displacement bypassing pits and flow out meter.

Equipment design issues

22. Instrumentation and displays for well monitoring not adequate
23. Weakness of the MGS design

24. BSR unable to shear pipe
25. BSR blades on indestructible joint
26. Weakness of the BSR design.

The above mentioned causes are arranged in several groups of different type, area of origin and importance. Their numbering corresponds to that used in Cause Map (Step 2, Pages 1 – 8). These causes and corresponding solutions are briefly discussed below.

Safety management and safety culture (Causes 1 – 7)

Analysis of risks and risk awareness

Companies involved in deepwater oil drilling must have in place strict policies requiring rigorous analysis and proof that less-costly alternatives are in fact equally safe (Cause 2). This recommendation also applies to current practice of making *ad hoc* changes during well development and completion without evaluation of the related risk (Cause 6). When implemented successfully, it would ensure that individual decision makers have a full awareness of the risk associated with the decision.

If BP had any such policies in place, it does not appear that its Macondo team adhered to them. Unless companies create and enforce such policies, there is simply too great a risk that financial pressures will systematically bias decision making in favour of time- and cost-savings (Cause 1).

Regulators need to create suitable framework that support such an approach. One of the important pre-conditions is clear formulation of health, safety and environmental objectives and establishing regulations that require operators, drilling contractors and service companies to work together to meet these safety objectives.

Safety management system

The most significant failure at Macondo – and the clear root cause of the blowout – was a failure of industry management. Most, if not all, of the failures at Macondo can be traced back to underlying failures of management and communication. Better management of decision making processes within BP and other companies, better communication within and between BP and its contractors, and effective transfer of information among key engineering and rig personnel would have prevented the Macondo incident (Causes 4, 5, and 7).

BP and other operators must have effective systems in place for integrating the various corporate cultures, internal procedures, and decision making protocols of the many different contractors involved in drilling a deepwater well.

The management system has to clearly define the roles and responsibilities for all parties involved in a given project (operator, drilling contractor and service companies) for health, safety and environmental protection. It should provide detailed project specific information to be shared by key personnel regardless of whether they are employed by the operator, the drilling contractor, or a service company. The system has to facilitate the management of change process and serve as a mechanism to communicate the implications of programme changes to all key personnel.

Safety culture

It is also critical that companies implement and maintain a pervasive top-down safety culture that reward employees and contractors who take action when there is a safety concern even though such action costs the company time and money (Causes 1 and 3).

Long-term proactive improvement programme that ensure effective learning from experience is an integral element of an effective risk management approach reflecting a safety culture (Cause 4). In such a programme “near misses” should provide opportunities to improve, and the reporting of errors, omissions, and questionable results should be highly encouraged. The regulators should establish practices and standards that foster continuous improvement in safety culture within the industry.

Regulatory oversight (Causes 8 – 10)

Regulatory approach

Government agencies[3] that regulate offshore activity should reorient their regulatory approaches to integrate more sophisticated risk assessment and risk management practices into their oversight of energy developers operating offshore (Cause 8). They should shift their focus from prescriptive regulations covering only the operator to a foundation of augmented prescriptive regulations, including those relating to well design and integrity, supplemented by a proactive, risk-based performance approach that is specific to individual facilities, operations, and environments[4].

This would be similar to the "safety case" approach that is used in the North Sea, which requires the operator and drilling rig owners to assess the risks associated with a specific operation, develop a coordinated plan to manage those risks, integrate all involved contractors in a safety management system, and take responsibility for developing and managing the risk management process.

Regulations and standards

The regulator agencies working with the International Regulators' Forum and other organizations, Congress and the DOI should identify those drilling, production, and emergency-response standards that best protect offshore workers and the environment, and initiate new standards and revisions to fill gaps and correct deficiencies.

Criteria for high-risk wells and develop methodology to assess those risks should be identified. This process should include input from broad group of experts. Furthermore, the DOI should develop in-house competence to perform such sophisticated risk assessments (Cause 10).

Such evaluations could guide the transition to a system where all operators and contractors are required to demonstrate an integrated, proactive, risk management approach prior to leases being granted or receiving permits for exploration wells and major development projects.

Coordinated, inter-agency research effort will be needed to develop safer systems, equipment, and practices to prevent failures of both design and equipment in the future. The federal government has relevant expertise in areas that could and should be transferred to the offshore industry.

More detailed requirements for incident reporting and data concerning offshore incidents and "near misses" are needed. Such data collection would allow for better tracking of incidents and stronger risk assessments and analysis. Such reporting should be publicly available and should apply to all offshore activities. In addition, DOI, in cooperation with the International Regulators Forum, should take the lead in developing international standards for incident reporting in order to develop a consistent, global set of data regarding fatalities, injuries, hydrocarbon releases, and other accidents. Sharing information as to what went wrong in offshore operations, regardless of location, is a key to avoiding such mistakes. Transparent information and data sharing within the offshore industry and among international regulators is critical to continuous improvement in standards and risk management practices.

Resources and staffing

To expand regulatory oversight and tighten safety requirements the regulatory agencies should be provided with adequate funding. Regulators to be more effective should be provided with the resources, personnel, and training. In the past these agencies were not adequately supported by industry, members of Congress, and several administrations. As a result, neither the regulations nor the regulators were asking the tough questions or requiring the demonstration of preparedness that could have avoided the Macondo disaster.

---

[3] The Mineral Management Service (MMS) that was the federal agency primarily responsible for regulating the safety of offshore drilling at the time of the Macondo well accident. Since October 1, 2011 the federal entity responsible for safety and environmental oversight of offshore oil and gas activities is the Bureau of Safety and Environmental Enforcement (BSEE).

[4] Proactive, goal-oriented risk management system similar to the systems used in the North Sea by the United Kingdom and Norway has already been instituted by DOI. Implementation of Safety and Environmental Management System (SEMS) in 30 CFR 250 (Federal Register, Vol. 75, No 199, Oct. 15, 2010) began on November 15, 2011.

The regulator should have a formal training and certification program for its inspectors. The extent of training of key personnel and decision makers in regulatory agencies has to be consistent with the complexities and risks of deepwater drilling. It is also essential that there is better opportunity for higher education and career advancement for inspectors. Individuals involved in regulatory oversight should have qualifications that are appropriate for meeting the challenges of the offshore drilling industry.

Procedures and training (Causes 11 – 16)

Procedures

The Macondo well accident identified several procedures that appear to be inadequate or lacking and require improvement. These include requirements for conducting cement bond log (Cause 11), procedure for conducting negative-pressure test (Cause 12), procedure on well monitoring (Cause 13), and emergency procedure for situations that involve loss of well integrity (Cause 14).

These procedures should be carefully reviewed and re-worked. They should clearly define mandatory practices and specify roles and accountabilities for the personnel involved. Procedures should be detailed enough to specify operational steps and decision points as well as the related criteria.

Procedures related to tests should include definition of success/failure criteria for the test. Procedures for operations that are more complex and carried out infrequently should be more detailed to compensate for unfamiliarity. So far there was a high reliance on leadership and know-how of the crew. However, the procedures that were available were guidelines only and did not provide enough detail. For instance, the procedure on negative-pressure test did not specify bleed volumes or give success/failure criteria.

While initial well design decisions undergo a serious peer review process and changes to well design are subsequently subject to a management of change (MOC) process, changes to drilling procedures in the weeks and days before implementation were typically not subject to any such peer-review or MOC process. At Macondo, such decisions appear to have been made by the BP Macondo team in ad hoc fashion without any formal risk analysis or internal expert review. This appears to have been a key causal factor of the blowout. Such practices are not acceptable and have to be eliminated.

These temporary abandonment procedures should be thoroughly and rigorously vetted earlier in the design process. It does not appear that the changes to the temporary abandonment procedures used at Macondo went through any sort of formal review at all.

Industry staff training

Standards for education, training, and professional certification of private-sector decision-making personnel involved in drilling operations in force at the time of the Deepwater Horizon accident were relatively minimal compared with other safety-critical industries, such as nuclear or chemical.

Personnel on the Deepwater Horizon MODU were mostly trained on the job, and this training was supplemented with limited short courses (such as 1 week of well control school every few years). While this appears to be consistent with industry standard practice and current regulations (such as 46 CFR 10.470 for OIMs), it is not comparable with other safety-critical industries such as nuclear power or chemical manufacturing. The appropriate qualifications of key personnel both on deepwater drilling rigs and ashore need to be assessed and improved, as needed, to provide for safe operations and protect the public interest.

Numerous decisions to proceed toward abandonment despite indications of hazard, such as the results of repeated negative-pressure tests, suggest an insufficient consideration of risk and a lack of operating discipline. The decisions also raise questions about the adequacy of operating knowledge on the part of key personnel. Improvement in the awareness of risks and risk management practices should help in resolving this issue.

The rig crew has to be trained adequately how to respond to escalating emergency situations, including the simulations and drills for such emergencies, and momentous decision to engage the blind shear rams or trigger the EDS.

During the Macondo well accident the crew had difficulty assessing the situation and understanding its significance. Appropriate training and job aids would have increased both the speed and accuracy

of identification that there was an influx of hydrocarbons and enhanced the probability of appropriate well control actions.

Process safety (Causes 17 – 21)

Investigation of causes of the Macondo well accident identified several process-specific decisions that contributed to the risk of blowout. They correspond to the causes 17 – 21 which are associated mostly with the implementation of temporary abandoning procedure. These specific issues should be carefully addressed in the development of appropriate internal procedures and Engineering Technical Practices.

Equipment design issues (Causes 22 – 26)

Investigation of causes of the Macondo well accident identified several design-specific concerns that contributed to the risk of blowout or had an impact on the severity of accident consequences. These weaknesses correspond to causes 22 – 26.

Instrumentation and displays used for well monitoring must be improved (Cause 22). An expert system decision aid should be used to provide timely warning of loss of well control to drillers on the rig (and ideally to onshore drilling monitors as well). If the warning is inhibited or not addressed in an appropriate time interval, autonomous operation of the blind shear rams, emergency disconnect system, general alarm, and other safety systems on the rig should occur.

Design of the MGS has to be evaluated with regard to consequences of its use beyond design basis, in particular, from the point of view of penetration of flammable gases to non-fire-protected zone through the HVAC system (Cause 23). Arrangement of gas detectors, automatic dampers, and alarms needs to be checked in this context, and eventual design changes introduced.

Cutting, sealing and separating capabilities of the BOP system should be specified in the regulations (Causes 24 - 25). Application of specific BOP systems in a well drilling project should be made consistently with the drilling environment to which they are applied and the rigs on which they are installed. Test and maintenance procedures should be established to ensure operability and reliability appropriate to their environment of application.

The use of two blind shear rams is also essential issue that needs resolution. Two blind shear rams give an extra measure of reliability, especially, if one shear ram hits on a joint connecting two drill pipes (Cause 25).

BOP as well as some other components that are critical to the safety of oil drilling operations should be required to be independently certified by a third party (such as a classification society) or by the relevant regulatory agency. At the time of the Macondo well accident the MMS did not directly oversee the initial and subsequent certifications of BOPs. Instead, the operator was to self-certify the BOP.

C.3. Bibliography for Annex C

British Petroleum, "*Deepwater Horizon Accident Investigation Report*", Sept. 8, 2010.

"*Interim Report on Causes of the Deepwater Horizon Oil Rig Blowout and Ways to Prevent Such Events*", National Academy of Engineering (NAE) and the National Research Council (NRC), prepared for U.S. Department of the Interior, November 16, 2010.

"*Macondo Well Deepwater Horizon Blowout, Lessons for Improving Offshore Drilling Safety*", National Academy of Engineering (NAE) and the National Research Council (NRC), prepared for U.S. Department of the Interior, Final Report. http://www.nap.edu/openbook.php?record_id13273

"*Deepwater, The Gulf Oil Disaster and the Future of Offshore Drilling*", Report to the President, National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling, January 2011.

Hubbard, A., Embrey, D., "*Deepwater Horizon – Summary of Critical Events, Human Factors Issues and Implications*", ©Human Reliability Associates Ltd, Sept. 23, 2010.

"*Oil Spill Reaches Mississippi River*". CBS News. 29 April 2010. Retrieved 29 April 2010.

"*Weekly Address: President Obama Establishes Bipartisan National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling*" (Press release). The Whitehouse. 2010-05-22. Retrieved 2010-06-01.

Oil Spill Commission, Chief Counsel's Report, http://www.oilspillcommission.gov/chief-counsels-report.

"*Oil spill: BP 'did not sacrifice safety to save money*"'. BBC. 9 November, 2010. Retrieved 12 November 2010.

"*Gulf oil spill: President's panel says firms complacent*". BBC. 9 November, 2010. Retrieved 12 November 2010.

Leo King (12 November 2010). "*Deepwater Horizon modelling software showed BP cement conditions unstable*". Computerworld UK. Retrieved 12 November, 2010.

David Barstow, Laura Dodd, James Glanz, Stephanie Saul and Ian Urbina "*Regulators Failed to Address Risks in Oil Rig Fail-Safe Device*", New York Times, June 20, 2010.

© ENCO

10 Annex D. List of Participants

Workshop Day 1

#	NAME (Alphabetical)	INSTITUTION
1.	Mr. ATHANASSIOU Georgios	University of Kassel
2.	Mr. BERG Johannes	TÜV NORD AG Head of Brussels Office
3.	Mr. BERNTSEN Marcel	COVRA N.V.
4.	BOLOGNESE, T.	EC DG ENER
5.	Ms. BROECKER Annette	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH Forschungszentrum
6.	Mr. BUET Baptiste	AREVA
7.	Mr. DEFFRENNES Marc	EC, DG Energy
8.	Mr. DELATTRE Dominique	IAEA Department of Nuclear Safety and Security
9.	Mr. DE ROOVERE Willy	Federal Agency for Nuclear Control Belgium
10.	Mr. FOUREST, Bernard	
11.	Mr. FUZER Jiri	CEZ European Affairs Department
12.	Mr. GARRIBA Massimo	EC, DG ENER
13.	Ms. GRUNERT Astrid	IACS
14.	Mr. GUANZIROLI Gianluigi	Alitalia, Safety Manager, Sicurezza Volo
15.	Mr. HILDEN Wolfgang	EC DG ENER
16.	Mr. HOLLNAGEL Erik	ENCO
17.	Ms. HUGUET-MOUSTAINE Agnes	AREVA, Nuclear & Renewable Energies
18.	Mr. IFTINCA Artur Cezar	OMV, Safety Expert
19.	Mr. JACKOWSKI Tomasz	Polish National Research Centre for Nuclear Research
20.	Mr. KREMER Laurent	Direction de l'Aviation Civile Luxembourg
21.	Ms. KRILIC Tatjana	IMO
22.	Ms. KROHN Sofia Bodil	Norsk olje&gass
23.	Mr. LACHAUME Jean-Luc	ASN
24.	Mr. LIGNINI Franck	AREVA
25.	Mr. MALINGE Yannick	AIRBUS

26.	Mr. MCGOWAN Paul	Commission For Energy Regulation Ireland
27.	Mr. MERENS Marco	ICAO (International Civil Aviation Organization), Safety Data Analysis Officer
28.	Mr. MEYNEN Friedrich	ENSI (Swiss Federal Nuclear Safety Inspectorate)
29.	Mr. MURTAGH Eamonn	Commission For Energy Regulation Ireland
30.	Mr. NOLLET Jos	NSA Netherlands, Senior Inspector
31.	Mr. NORDGARD Alfred	Norwegian Oil Industry Association
32.	Mr. PAULY Jan	E.ON
33.	Ms. POPA Ioana	ENCO
34.	Mr. POUGET-ABADIE Xavier	EDF, Délégué Relations Internationales avec les Autorités de Sûreté
35.	Mr. PRASIL Jan	CEZ, European Affairs Department
36.	Mr. RÄTZKE Christian	WNA Cordel
37.	Mr. REGO Fransico	US Coast Guard
38.	Mrs. REMOND	ENSI (Swiss Federal Nuclear Safety Inspectorate)
39.	Mr. SCHMID Juerg	ENCO
40.	Mr. SCHWEBS Rune	PSA, Petroleum Safety Authority Norway
41.	Mr. SKJONG Rolf	Det Norske Veritas AS
42.	Mr. STORBECK Jörg	EnBW Energie Baden, Management Sector Technics Head of Nuclear Generation
43.	Mr. STRÄTER Oliver	Kassel University ***(presentation of software)***
44.	Mr. STRUCIC Miodrag	EC, JRC Petten
45.	Mr. STURM Jochen	Se-Engineering GmbH
46.	Mr. TOMIC Bojan	ENCO
47.	Mr. VAN DER BORST Mario	RWE
48.	Ms. VELICU Oana	ENCO
49.	Mr. VERWEIJ Bert	Transport Inspectorate, Department of Nuclear Safety Netherlands
50.	Mr. VIGNE Serge	EC, DG Energy
51.	Mr. VILLADONIGA José Ignacio	Tecnatom
52.	Mr. WAESSMAN Per-Olof	Vattenfall, Safety and licensing Nuclear Department
53.	Mr. VINCENT John	European Aviation Safety Agency, Deputy Director for Strategic Safety and Head of Safety Analysis

54.	Mr. WELBERGEN Jeroen	COVRA
55.	Ms. YLIKNUUSSI, Niina	EC DG ENER

* fields marked in orange signify keynote speakers and/or Enco staff

Workshop Day 2

#	NAME (Alphabetical)	INSTITUTION
1.	Mr. ATHANASSIOU Georgios	University of Kassel
2.	Mr. BERNTSEN Marcel	COVRA N.V.
3.	BOLOGNESE, T.	EC DG ENER
4.	Ms. BROECKER Annette	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS) mbH Forschungszentrum
5.	Mr. BUET Baptiste	AREVA
6.	Mr. DEFFRENNES Marc	EC, DG Energy
7.	Mr. DELATTRE Dominique	IAEA Department of Nuclear Safety and Security
8.	Mr. DE ROOVERE Willy	Federal Agency for Nuclear Control Belgium
9.	Mr. FOUREST, Bernard	
10.	Mr. FUZER Jiri	CEZ European Affairs Department
11.	Gress, P.	EC DG ENER
12.	Mr. GUANZIROLI Gianluigi	Alitalia, Safety Manager, Sicurezza Volo
13.	Mr. HOLLNAGEL Erik	ENCO
14.	Ms. HUGUET-MOUSTAINE Agnes	AREVA, Nuclear & Renewable Energies
15.	Mr. IFTINCA Artur Cezar	OMV, Safety Expert
16.	Mr. JACKOWSKI Tomasz	Polish National Research Centre for Nuclear Research
17.	Mr. KREMER Laurent	Direction de l'Aviation Civile Luxembourg
18.	Ms. KRILIC Tatjana	IMO
19.	Ms. KROHN Sofia Bodil	Norsk olje&gass
20.	Mr. MALINGE Yannick	AIRBUS
21.	Mr. MCGOWAN Paul	Commission For Energy Regulation Ireland
22.	Mr. MERENS Marco	ICAO (International Civil Aviation Organization), Safety Data Analysis Officer

23.	Mr. MEYNEN Friedrich	ENSI (Swiss Federal Nuclear Safety Inspectorate)
24.	Mr. MURTAGH Eamonn	Commission For Energy Regulation Ireland
25.	Mr. NOLLET Jos	NSA Netherlands, Senior Inspector
26.	Mr. NORDGARD Alfred	Norwegian Oil Industry Association
27.	Mr. PAULY Jan	E.ON
28.	Ms. POPA Ioana	ENCO
29.	Mr. POUGET-ABADIE Xavier	EDF, Délégué Relations Internationales avec les Autorités de Sûreté
30.	Mr. PRASIL Jan	CEZ, European Affairs Department
31.	Mr. RÄTZKE Christian	WNA Cordel
32.	Mr. REGO Fransico	US Coast Guard
33.	Mrs. REMOND	ENSI (Swiss Federal Nuclear Safety Inspectorate)
34.	Mr. SCHMID Juerg	ENCO
35.	Mr. SCHWEBS Rune	PSA, Petroleum Safety Authority Norway
36.	Mr. SKJONG Rolf	Det Norske Veritas AS
37.	Mr. STORBECK Jörg	EnBW Energie Baden, Management Sector Technics Head of Nuclear Generation
38.	Mr. STRÄTER Oliver	Kassel University ***(presentation of software)***
39.	Mr. STRUCIC Miodrag	EC, JRC Petten
40.	Mr. STURM Jochen	Se-Engineering GmbH
41.	Mr. TOMIC Bojan	ENCO
42.	Mr. VAN DER BORST Mario	RWE
43.	Ms. VELICU Oana	ENCO
44.	Mr. VERWEIJ Bert	Transport Inspectorate, Department of Nuclear Safety Netherlands
45.	Mr. VIGNE Serge	EC, DG Energy
46.	Mr. VILLADONIGA José Ignacio	Tecnatom
47.	Mr. WAESSMAN Per-Olof	Vattenfall, Safety and licensing Nuclear Department
48.	Mr. VINCENT John	European Aviation Safety Agency, Deputy Director for Strategic Safety and Head of Safety Analysis
49.	Mr. WELBERGEN Jeroen	COVRA
50.	Ms. YLIKNUUSSI, Niina	EC DG ENER

11 Annex E. Workshop Agenda

How to Improve Safety in Regulated Industries

What Could We Learn From Each Other

Start	End	AGENDA
		Tuesday, October 16th, 2012 ***(Ampere Room, Bâtiment Joseph Bech, 5, rue Alphonse Weicker, Luxembourg)***
9:00	9:05	**Welcome, EC DG ENER**
9:05	9:20	**Introduction to Workshop, Purpose, and Goals - Chairman Prof. Erik Hollnagel, Univ. of Southern Denmark**
9:20	**10:50**	**Game changer events, analyzed by non-parties**
9:20	09:50	**Fukushima NPP – Mr. Friedrich Meynen, ENSI**
9:50	10:20	**Deepwater Horizon Drilling Rig – Mr. Frank Rego, US Coast Guard**
10:20	10:50	**Air France Flight 447 – Mr. Juerg Schmid, ENCO**
10:50	11:05	Coffee Break
11:05	**11:20**	**The Safety NET Concept**
11:05	11:20	**Safety NET: the concept of mutually supportive interactions - Prof. Erik Hollnagel, Univ. of Southern Denmark**
11:20	**12:10**	**Keynote safety challenges – Aviation**
11:20	11:40	**Vendor's safety concepts - Mr. Yannick Malinge, Airbus**
11:40	12:00	**Regulator's position on changing technologies and operational concepts - Mr. John Vincent, EASA**
12:00	12:10	**Questions to presenters**
12:10	**13:00**	**Keynote safety challenges – Offshore**
12:10	12:30	**Operator's safety responsibilities – Mr. Alfred Nordgård, Norwegian Oil Industry Association**
12:30	12:50	**Going beyond compliance – How authority strategies may contribute to safety – Mr. Rune Schwebs, PSA**
12:50	13:00	**Questions to presenters**
13:00	14:00	**Lunch** *(Provided, Ampere Foyer)*
14:00	**15:10**	**Keynote safety challenges – Nuclear**
14:00	14:20	**Vendor role in advancing safety - Mr. Franck Lignini, Areva**
14:20	14:40	**Operator's responsibility for safety - how is it implemented - Mr. Jan Pauly, E.ON**
14:40	15:00	**Regulatory Oversight and its role in assuring safety – Mr. Jean-Luc Lachaume**
15:00	15:10	**Questions to presenters**
15:10	**17:00**	**Supranational Frameworks**
15:10	15:30	**IAEA standards and their role - Mr. Dominique Delattre, IAEA**
15:30	15:50	Coffee Break/**Demonstration: Safety scanning tool, Prof. O. Sträter, Kassel University**
15:50	16:10	**Integrated Safety Analysis and USOAP - Mr. Marco Merens, ICAO**
16:10	16:30	**IMO MSAS concepts and experience so far - Ms. Tatiana Krilic, IMO**
16:30	16:50	**EC framework for nuclear safety – Mr. Massimo Garriba, EC DG ENER**
16:50	17:00	**Questions to presenters/Short break**
17:00	17:10	Short Break

17:00	**18:00**		**Experience in cross cutting**
17.10	17.30		**Lessons Learned from OPEX Management in Hazardous Industries – Mr. Miodrag Sturcic, EC JRC**
17.30	17.50		**Aviation certification and improvement of safety - what can nuclear learn - Mr. Christian Raetzke, WNA CORDEL and ENEF ERDA**
17:50	18:00		**Questions to presenters**
18.00			**Networking event: Cocktail offered by organizers** *(Ampere Foyer)*

Start	End		AGENDA			
Wednesday, October 17th, 2012 (Ampere Room and Foyer, Bâtiment Joseph Bech, 5, rue Alphonse Weicker, Luxembourg)						
9:00	**12:00**		**Identifying the Way Forward** *(Breakout sessions)*			
			GROUP 1 **How to establish a challenging attitude to enhance safety? Drivers and the roles in achieving, maintaining and strengthening safety** *Group lead: J. Villadoniga* *Rapporteur: O. Velicu* *(TBD)*	**GROUP 2** **How to strengthen the safety NET? Interaction of vendors, operators and regulators, confrontation vs. collaboration, role of supranational regulation** *Group lead: G. Guanziroli* *Rapporteur: I. Popa* *(TBD)*	**GROUP 3** **What is the impact of major events on safety thinking/concept – are those game changers? Lessons for vendors, operators and regulators** *Group lead: W. de Roovere* *Rapporteur: M. van den Borst* *(TBD)*	**GROUP 4** **What can we learn from each other? Practical aspects and learning field from other industries, what is "transferable" and what not** *Group lead: R. Skjong* *Rapporteur: B. Tomic* *(TBD)*
			Coffee Break (to be taken at the discretion of the groups)			
			A challenging attitude **Summary**	**The safety NET** **Summary**	**Impact of major events** **Summary**	**Practical aspects and learning field** **Summary**
12:00	13:00		**Lunch** *(Provided, Ampere Foyer)*			
13:00	**15:30**		**Summary Session**			
13:00	13:10		**Findings – Challenging attitude – Mr. J. Villadoniga, Group 1**			
13:10	13:30		**Discussion**			
13:30	13:40		**Findings – The safety NET – Mr. G. Guanziroli, Group 2**			
13:40	14:00		**Discussion**			
14:00	14:10		**Findings – Impact of major events - Mr. W. de Roovere, Group 3**			
14:1	14:3		**Discussion**			

0	0		
14:30	14:40		**Findings – Learning field – Mr. R. Skjong, Group 4**
14:40	15:00		**Discussion**
15.00	15.30		**Joint discussion on all topics**
15:30	15:45		Coffee Break
15:45	**16:30**		**Plenary Discussion**
15:45	16:15		**Highlights: What did we learn, what could we do better (plenary discussion) – Workshop Chairman Prof. Erik Hollnagel, University of Southern Denmark**
16:15	16:30		**Conclusions of the meeting, ideas to take home, action points – Mr. Bojan Tomic, ENCO**
16:30			**ADJOURN**

12 Annex F. Workshop Presentations

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*):

00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

More information on the European Union is available on the Internet (http://europa.eu).

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2013

ISBN 978-92-79-29934-6
doi: 10.2768/23154

© European Union, 2013
Reproduction is authorised provided the source is acknowledged.

KO-NA-25-979-EN-N

ISBN 978-92-79-29934-6
doi:10.2768/23154