Integrating Safety into an Engineering Contractor's System Engineering process using the guidelines of STAMP (Systems-Theoretic Accident Model and Processes)

or

Evaluating Project Safety (System Engineering and Safety Management) in an Organization

Lorena Pelegrín

Registration Number 071240048

A thesis submitted in partial fulfilment of the requirements for the degree of

Safety, Risk and Reliability Engineering, MSc

Thesis Supervisor: Dr. Nancy Leveson, Professor of Aeronautics and Astronautics and Engineering Systems, Massachusetts Institute of Technology

Heriot-Watt University

School of the Built Environment

August 2012

Declaration:

I hereby confirm that this dissertation is my own work.

Signature **Date**

DECLARATION

I Lorena Pelegrín confirm that this work submitted for assessment is my own and is expressed in my own words. Any uses made within it of the works of other authors in any form (e.g. ideas, equations, figures, text, tables, programmes) are properly acknowledged at the point of their use. A full list of the references employed has been included.

Signed: …………………………….

Date: ……………………………......

Table of Contents

List of Tables and Diagrams

Acknowledgements

I would like to thank Professor Nancy Leveson of Massachusetts Institute of Technology, my thesis advisor, for having accepted supervising this thesis and for letting me join the Partnership for Systems Approaches to Safety. I would also like to thank her for having showed me with her research and last book that there is more to safety than what is practiced today in the industry, an inspiration I was desperately looking for.

Many thanks to Dr. Pauline Thompson of Heriot-Watt University Edinburgh, Director of the Safety, Risk and Reliability Program, for always answering my questions while studying, and for letting me write this thesis with Professor Nancy Leveson.

Thanks to ILF Consulting Engineers for sponsoring this work and my studies in the last years.

My gratitude and respect to Christian Heinz, Business Area Director of ILF Consulting Engineers, for believing in me, for supporting my studies in the last years, and for all the interesting discussions and projects he has got me into.

I would also like to thank my colleagues who found time for the discussions and answers of my questions during the initial status review performed for this thesis.

A special thanks to Professor Jesús Larralde-Muro of California State University Fresno, for introducing me to the world of research years ago, and for supporting me in continuing studying with this MSc.

I am deeply grateful to my parents Antonio Pelegrín and Marián Álvarez for everything they have done for me. A special thanks to my uncle Federico Álvarez, who got interested in this quest, and advised me to follow my dreams. The last thanks to my mom for believing in me, for her unconditional support and for pushing me to go beyond.

Abstract

ENGINEERING CONTRACTOR is a group of engineering and consulting companies providing services worldwide in the fields of Oil & Gas, Water & Environment, Energy & Climate Protection and Transport & Structures. Because currently there is no consolidated system engineering process which includes designing for safety systematically, and the top management of EC has understood the responsibility of EC in the safety of the systems they engineer, the present thesis was proposed.

An initial review on how safety is addressed in the system engineering process in EC was performed. The fundamentals of using STAMP (Systems-Theoretic Accident Model and Processes) in system engineering were used as guidelines to check against. The hypotheses included that EC varies widely the approach to safety depending on the different client requirements and involvement of individuals, and that the results of safety-related activities have a weak impact on the system design and often are used as instruments to legitimize a design rather than to improve the safety of the system. The survey confirmed the hypotheses to a great extent.

After the initial review, the results were analyzed in terms of identification of current practice and feasibility of STAMP implementation in EC. A case on implementation of the new techniques to a project example was also developed for illustration purposes. Finally, high-level guidelines and a strategy for implementation of STAMP in EC were derived.

This work has concluded that the use of STAMP principles and the guidelines given in Leveson's "Engineering a Safer World" provide a comprehensive, detailed and useful frame for evaluating how an organization designs for safety and for defining measures specifically tailored to an organization. This work has also demonstrated that while a fundamental departure from traditional safety engineering and hazard analysis techniques might seem a difficult campaign to undertake, it is possible to incorporate many elements of STAMP and STPA (Systems-Theoretic Process Analysis) in the short term with significant impact on how safety is designed into the system, and moreover with a by-product improvement in the efficiency of engineering management activities and the quality of the engineering work delivered.

Glossary of Terms

Engineering a Safer World

Leveson, N. G., 2011. Engineering a Safer World. Systems Thinking Applied to Safety. MIT Press, Engineering Systems Series. ISBN 978-0-262-01662-9, Jan 2012.

Safety

Absence of fatalities and injuries during system operation.

Limited definition for the purpose of this thesis derived from Leveson’s definition of safety as freedom from accidents (or loss).

Safety-related

Something which might influence safety, i.e. project activity which might influence the absence (or presence) of fatalities and injuries during system operation.

VISION

Heriot-Watt University's Virtual Learning Environment. It is a web-based integrated teaching and learning environment.

Nomenclature

A	Accident
BVS	Block Valve Station
CIS	Commonwealth of Independent States
COESD	Controlled Operation Emergency Shut Down
DEP	Design Engineering Practice
DEUDAN	DEUDAN Gas Pipeline which connects the German and Danish gas networks
EC	ENGINEERING CONTRACTOR
e.g.	An abbreviation of Latin “exempli gratia” e.g. is often used to introduce an example. It is sometimes pronounced as “for example”
EGIG	European Gas Pipeline Incident data Group
EPC	Engineering Procurement Construction
ESD	Emergency Shut Down
ESIA	Environmental and Social Impact Assessment
ETP	Engineering Technical Practices
FEED	Front End Engineering Design
FFS	Fire Fighting System
F&G	Fire and Gas Detection System
FPS	Flow Path Supervision
G	Goal
GB	Geschäftsbereich (=Business Unit)
GB-A	Business Unit-Acquisition
GB-B	Business Unit-Business Services
GB-C	Business Unit-Gas Compressor Stations
GB-E	Business Unit- Electrical Power Systems
GB-I	Business Unit- Instrumentation, Automation and Telecom
GB-L	Business Unit-Tank Farms and Terminals
GB-M	Business Unit-Pipeline Systems
GB-P	Business Unit-Project Management
GB-S	Business Unit-Process Facilities
GB-U	Business Unit-Upstream
HSE	Health, Safety and Security, and Environment protection
HAZID	Hazard Identification study
HAZOP	Hazard and Operability study

ICSS	Integrated Control and Safety System
IDS	Intrusion Detection System
i.e.	An abbreviation of Latin “id est”
	i.e. is often used to explain or clarify a statement. It is sometimes pronounced as “that is”
IEC	International Electrotechnical Commission
IMS	Integrated Management System
IOS	Integrated Open Season
IT	Information Technology
LCC	Local Control Centre
LDS	Leak Detection System
LOC	Loss Of Containment
MCC	Main Control Centre
MTA	Million Tons per Annum
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
Nm^3/h	Normal Cubic Meters per Hour
OREDA	Offshore Reliability Data
PCS	Pressure Control System
PID	Piping and Instrumentation Diagram
PMC	Project Management Consultancy
QRA	Quantitative Risk Assessment
SCADA	Supervisory Control and Data Acquisition
SCS	Station Control System
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
STAMP	Systems-Theoretic Accident Model and Processes
STPA	Systems-Theoretic Process Analysis
UCA	Unsafe Control Action
WAG	West-Austria Gas Pipeline

Project Planning Documents

This section slightly deviates from the list of Project Planning Documents proposed in the report template downloaded by the Author from VISION. The planning elements and information provided below are considered sufficient for the purpose of this thesis, given the reduced organizational complexity faced.

1. Project Activities

The following activities have been planned to be performed sequentially as far as practicable.

- Prepare, discuss and approve thesis proposal
- Study “Engineering a Safer World. Systems Thinking Applied to Safety”
- Perform Initial Status Review
- Perform analysis of STAMP steps
- Apply STAMP steps to a Project Example
- Define high-level guidelines for a new system engineering process which integrates safety
- Define a strategy for implementation of STAMP into EC’s system engineering process
- Generate Conclusions
- Think about next steps
- Prepare report

2. Time Frame

January 2012 – July 2012.

3. Roles and Responsibilities

- Author

  Lorena Pelegrín, ILF Consulting Engineers. Consultant Loss Prevention and Risk Management. Based in Munich, Germany.

  Write the thesis and coordinate requirements of supervisors.

- Thesis Supervisor

  Dr. Nancy Leveson, Massachusetts Institute of Technology. Professor, Aeronautics and Astronautics and Engineering Systems. Author of “Engineering a Safer World. Systems Thinking Applied to Safety” (published by MIT Press January 2012) where STAMP is explained. Based in Boston, MA USA.

  Provide guidance on application of the techniques described in her book and ensure the work complies with the principles of STAMP.

- ILF Supervisor

  Christian Heinz, ILF Consulting Engineers. Director, Business Unit Pipeline Systems. Based in Munich, Germany.

  Ensure the work delivers an improved and usable way for ILF to consider safety in the System Engineering processes.

- Heriot-Watt University Supervisor

  Dr. Pauline Thompson, Heriot-Watt University. Programme Director, MSc Safety Risk and Reliability Engineering. Based in Edinburgh, UK.

  Ensure the work complies with Heriot-Watt dissertation quality requirements.

1 Introduction

1.1 Problem

ENGINEERING CONTRACTOR is a group of engineering and consulting companies providing services worldwide in the fields of (i) Oil & Gas, (ii) Water & Environment, (iii) Energy & Climate Protection and (iv) Transport & Structures. See overall organization of the EC Group in Figure 1 below.

The core business field of EC Company(further on referred to in this document as EC) is Oil & Gas specializing in (i) Production Facilities for Oil & Gas, (ii) Pipeline Systems, (iii) Tank Farms and Underground Storage Facilities and (iv) Refineries and Petrochemical Plants.

Currently there is no consolidated system engineering process within EC which takes into consideration safety systematically. Isolated activities and studies are performed mainly driven by client requirements or involvement of individuals. The results of these activities and studies have a weak impact on the system design and often are used as instruments to legitimize a design rather than to improve the safety of the system. The general perception is that the so-called Safety Studies are costly activities that do not really add value to the product; this is also the perception of many clients. A survey or so-called Initial Status Review has been performed in the frame of this thesis which confirms these hypotheses to a great extent.

The Management of EC has understood the responsibility of EC in the safety of the systems they engineer and have defined as part of the so-called Strategic Goals for 2011 to “Integrate occupational health and safety, technical safety and environmental protection in the projects”. In the frame of the work to reach this goal, the present thesis has been proposed.

While a fundamental change towards designing for safety instead of checking the safety of the designs is not expected short term, it is still possible to introduce the “pro-active” approach of enforcing safety constraints in the designs as described by Leveson in “Engineering a Safer World. Systems Thinking Applied to Safety”.

1.2 Objective

EC’s objective is to obtain an improved and usable way for EC to consider safety in the system engineering process. Usable way is understood as a way which is simple and cost effective for EC. A usable way should also bring a reduction in paper and formalities burden, while effectively increasing awareness about safety. These are key requirements for the new process to find acceptability in the organization.

The thesis objective is to develop a new system engineering process integrating safety for EC using the guidelines of STAMP (Systems-Theoretic Accident Model and Processes).

Figure 1: Overall Organization of the EC Group, Status May 2011 [4] -deleted

1.3 Scope

The Scope of the new process for integrating safety into system engineering includes the facility lifecycle phases (i) Concept Selection and (ii) Basic Design. The initial phase of project identification or Feasibility phase (as defined by some operators) is not considered part of the system engineering process for the projects EC usually processes since the main focus is on productivity; therefore it is excluded from the scope of this new process and this thesis. The following phases of project execution—including detail design, facility operation and decommissioning (again as defined by some operators)— are also excluded from the scope of this work due to time constraints. Moreover it is considered that the engineering and design decisions to be performed during Concept Selection and Basic Design are more interesting (are of greater criticality) from the perspective of safety assurance because later in detail design organizations are reluctant to perform major changes on those designs even if significant hazards are identified. Therefore those early decisions have a key impact on the future safety of the system.

1.4 Approach

1.4.1 Initial Status Review

An initial review on how safety is addressed in the system engineering process in EC is performed. The fundamentals of using STAMP in system engineering are considered, but not explicitly referred to during the review sessions. The goal of this step is to learn about how EC addresses the safety issue during engineering. The hypothesis is that EC varies widely in the approach to safety depending on the client requirements rather than depending on system complexity.

1.4.2 Analysis of STAMP Steps

The elements of using STAMP are analyzed in terms of (i) Current EC practice, (ii) Feasibility of step implementation in EC and (positive) by-products, (iii) Development of step for a Project Example (see below), (iv) Definition of high-level guidelines for implementation of step in EC.

1.4.3 Project Example

It is considered helpful (i) for illustration of the techniques and (ii) for developing the organization necessary to perform every step (i.e. trying/selecting resources including time), to apply the techniques to a project example.

The selected Project is “Oil Product Pipeline Komsomolsk – De Kastri”. The purpose of the Komsomolsk – De Kastri Oil Product Pipeline Project is to transport oil products (i) Diesel Fuel 2.7 MTA, (ii) Naphtha 2.0 MTA and (iii) Jet Fuel 1.0 MTA produced in the Refinery Komsomolsk (located in Komsomolsk-on-Amur in Far East Russia) to other destinations in Far East Russia (Kamchatka, Chukchi Peninsula and Magadan) as well as to Pacific Rim Markets (China, Japan, Indonesia and possibly USA).

The current oil product transport scheme is from the Refinery Komsomolsk via railway to the Ports Vanino and Nakhodka. From there the oil products are delivered to Pacific

Rim Markets by tankers. See figures below (blue lines). The new planned transport scheme replaces most of the existing railway transport volume so that most of the oil products are transported via pipeline (approx. 330 km) from the Refinery Komsomolsk to the Port De-Kastri. See figures below (red lines). The overall intent is to improve oil product transport reliability with the new system.

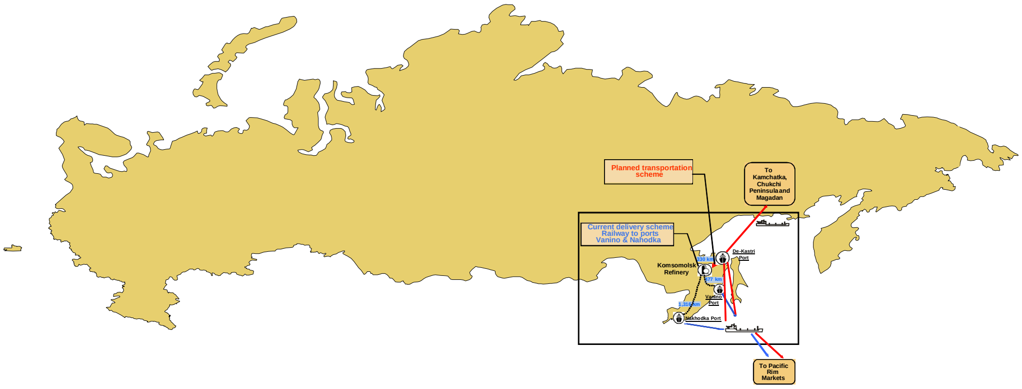

Planned transportation scheme
To Kamchatka, Chukchi Peninsula and Magadan
Current delivery scheme Railway to ports Vanino & Nahodka
Komsomolsk Refinery
De-Kastri Port
Vanino Port
Nakhodka Port
To Pacific Rim Markets

Figure 2: Oil Product Pipeline Komsomolsk-De Kastri Project – Overview location in the Russian Federation, adapted from [2]

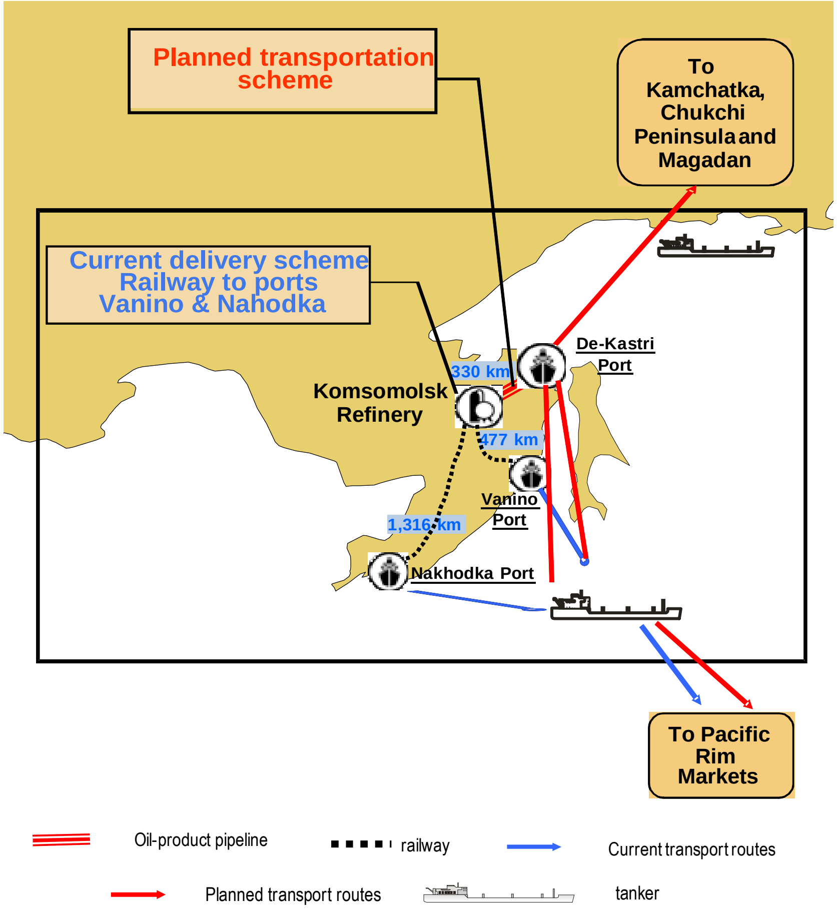


Figure 3: Oil Product Pipeline Komsomolsk-De Kastri Project – Detail current transportation scheme and planned transportation scheme, adapted from [2]

The new transportation system is planned to start operation by mid 2014 and foresees a period of operation of 30 years. Capital investment has been estimated in the order of 1 bn USD.

Design Institute has previously performed the so-called Investment Justification work for the Project. This is somehow equivalent to the system engineering work usually performed during the Concept Selection facility lifecycle phase. This work has been carried out strictly following Russian norms and standards as is common practice in the Russian Federation. Design Institute has been appointed as the General Designer in the Project and has coordinated the Investment Justification work.

Before continuing with the Basic Design work on the basis of the results of the Investment Justification, Design Institute has contracted EC to perform Concept Selection and Functional Design according to international best practice. The intent of Design Institute with this contract is to try to find better solutions which will be compared with the solutions of the previous Investment Justification. The scope of the contract includes (i) System optimization and selection (pipeline, pump stations, tank farms, batch sizes, loading facilities and multiproduct technology), (ii) Preparation of Process Flow Diagrams and Piping and Instrumentation Diagrams (PIDs) as well as operating philosophies and (iii) Definition and specification of key equipment. The only planned “classic” Safety Study as per contract scope is a HAZOP after preparation of PIDs.

This project is considered adequate for illustration of the techniques since it exhibits a medium size and degree of complexity so that it can be handled in the frame of the thesis.

1.4.4 Strategy for Integrating Safety into EC’s System Engineering process

Once the analysis of steps is completed and the high-level guidelines are distilled, then an action plan can be defined for implementation of STAMP into EC’s system engineering process.

2 Initial Status Review

This chapter describes the approach for performing an Initial Status Review on how safety is addressed in the system engineering process in EC. The fundamentals of using STAMP in system engineering have been considered, but not explicitly referred to during the review sessions. The goal of this step is to learn about how EC addresses the safety issue during engineering.

2.1 Review Organization

2.1.1 General

The review has been performed analyzing two aspects: (i) Business Units and (ii) Projects. Short interviews have been performed with Business Unit Directors of EC and Project Managers of a selection of representative projects respectively. Projects are developed by personnel under the responsibility of Business Unit Directors. This is usually referred to in EC as a Matrix Organization. The results of the interviews are analyzed for identification of established current practice and culture. This exercise provides information on how established processes and culture can realistically be changed for improvement through the use of STAMP principles in system engineering (i.e. "how far we can actually go on the implementation of STAMP principles as per today").

2.1.2 Business Units

2.1.2.1 General

Figure 4 below shows the Organization Chart of EC Company. EC Company is divided in ten Business Units. This structure is the result of company fast growth in the last ten years. Even if the names of the Business Units seem to be business field oriented, the structure is not truly business field or discipline oriented, but a mixture of both developed over the company history.

The company's Business Units traditionally involved in system design are GB-S (previously including GB-U), GB-M (previously including GB-C and GB-L) and GB-E (previously including GB-I) with remarkable dominance of GB-S (i.e. "the owners of the process") and GB-M (i.e. "the system designers and component specialists"). GB-E has been traditionally considered a support unit. The so-called New Business Units have been separated from the mother Business Units as specialization of departments gradually has become clear and the related business volume has increased making it simpler to be managed as a separate unit.

Due to the fast organic growth in the last years, concentrating on the development of business, it can be noted that there has not been a visible group in the organization established for safety. There is a so-called "Safety Expert" independent of the Business Units reporting to Managing Directors which is an occupational health and safety position for the workforce required by German Law and not involved in system design. Safety-related activities are neither a visible responsibility of a specific Business Unit performing system design, nor of a separate independent group.

Figure 4: Organization Chart ofEC Company, Status July 2011 [4] -deleted

The following sections describe the Business Units in terms of functions/departments together with remarks on the relevance for being subject of this Initial Status Review. Four Business Units have been considered relevant for Initial Status Review (i.e. GB-S Process Facilities, GB-U Upstream, GB-M Pipeline Systems and GB-I Instrumentation, Automation and Telecom). Business Unit Directors of identified relevant Business Units have been interviewed on the basis of the Checklist described below.

2.1.2.2 GB-S Process Facilities

Functions/departments include (i) Gas Storage, (ii) Gas Processing, (iv) Simulation & Process Services and (v) HVAC.

Old Business Unit. Previously also including GB-U projects and resources. Leads system design of downstream process facilities. Traditional hazard analyses such as HAZID, HAZOP and QRA have been performed in this unit in the past. Also safety-related engineering work is performed in this unit such as preparation of isolation and blow down philosophies or operation, control and safety shut-down philosophies.

This Business Unit is considered relevant for Initial Status Review.

2.1.2.3 GB-U Upstream

Functions/departments include (i) Upstream Onshore, (ii) Upstream Offshore and (iii) Upstream Oil / Water Processing.

New Business Unit. Part of GB-S up to 2010. Carries out mainly reviews of designs performed by other organizations of upstream process facilities. Hazard analyses are requested to either GB-S or GB-M.

This Business Unit is considered relevant for Initial Status Review.

2.1.2.4 GB-C Gas Compressor Stations

Functions/departments include (i) System Design Compressor Stations, (ii) Mechanical Equipment/Rotating Equipment and (iii) Piping Design & Plant Layout.

New Business Unit. Part of GB-M up to 2010. Leads system design of gas compressor stations. Hazard analyses are requested to either GB-S or GB-M.

This Business Unit is not considered relevant for Initial Status Review.

2.1.2.5 GB-M Pipeline Systems

Functions/departments include (i) Onshore & Offshore Pipeline Technology and System Design, (ii) Machinery & Mechanical Components, (iii) Routing and Authority Engineering, (iv) Rehabilitation & Pipeline Technology and (v) Management Capital Projects.

Old Business Unit. Previously also including GB-C and GB-L projects and resources. BU leading projects with highest turnover in EC Company and the EC Group. Leads system design of pipeline systems including tank farms and terminals. Design of gas compressor stations is now requested to GB-C. Performs traditional hazard analyses such as HAZID, HAZOP and QRA and is responsible for design of safety-critical systems such as fire fighting.

This Business Unit is considered relevant for Initial Status Review.

2.1.2.6 GB-L Tank Farms and Terminals

Functions/departments include (i) System Design Storage & Terminals.

New Business Unit. Part of GB-M up to 2009. This unit is organized as an acquisition and project supervision unit only. It has no own engineering capabilities and requests those from the other BU or from low cost engineering countries, like EC subsidiaries in Romania or the Czech Republic.

This Business Unit is not considered relevant for Initial Status Review.

2.1.2.7 GB-I Instrumentation, Automation and Telecom

Functions/departments include (i) Instrumentation & Station Control, (ii) Central Control/SCADA, (iii) Telecom & IT Systems and (iv) EC IT Services.

New Business Unit. Part of GB-E up to 2011. However remains mainly as a support unit. SIL Assessments have been traditionally performed in this unit. A lot of safety-related system and sub-system work is performed such as preparation of operation, control and safety shut-down philosophies, safety-critical systems such as fire and leak detection, etc.

This Business Unit is considered relevant for Initial Status Review.

2.1.2.8 GB-E Electrical Power Systems

Functions/departments include (i) Industrial Plants, (ii) Transmission and Distribution, (iii) Photovoltaic and (iv) Industrial Energy Efficiency.

Old Business Unit. Previously also including GB-I projects and resources. Has developed own business field competence in the recent years and continues to support other units.

This Business Unit is not considered relevant for Initial Status Review.

2.1.2.9 GB-P Project Management

Functions/departments include (i) Project Management services, (ii) Procurement Services, (iii) Construction Supervision, (iv) PMC services and (v) EPC Management Consultancy.

Project support unit. Not directly involved in system design. Small group in the organization having no involvement in system design, i.e. opinion of other Business Units, for which GB-P is performing a service, usually prevails.

This Business Unit is not considered relevant for Initial Status Review.

2.1.2.10 GB-A Acquisition

Project acquisition unit. Not involved in system design.

This Business Unit is not considered relevant for Initial Status Review.

2.1.2.11 GB-B Business Services

Administrative unit. Not involved in system design.

This Business Unit is not considered relevant for Initial Status Review.

2.1.3 Projects

2.1.3.1 General

The following sub sections introduce the projects which have been reviewed in the frame of the Initial Status Review. These projects are considered representative. Project Managers have been interviewed on the basis of the Checklist described below. The project descriptions below have been reproduced from available project documentation and information publicly available.

2.1.3.2 Project 1

The purpose of the Burgas – Alexandroupolis Oil Pipeline Project is to carry crude oil produced in Russia, Kazakhstan and Azerbaijan to destinations in the European Union, North America and other international markets. For the additional crude oil production expected in near future in these CIS countries the Burgas – Alexandroupolis Crude Oil Pipeline serves as transport way additional to the shipping of oil through the Bosporus Straits which faces physical limitations and environmental threats. The crude oil will be transported by tankers from oil ports in the Black Sea to Burgas (Bulgaria) and from there, via the pipeline system, to Alexandroupolis (Greece). In Alexandroupolis it will be loaded on tankers that will take the crude oil to its final destination.

Further information publicly available may be accessed at [5].

The scope of the project relevant for this Initial Status Review is Conceptual Design, Functional Design and Basic Design.

2.1.3.3 Project 2

The purpose of the Crystal Gas Storage project is to construct a storage facility in Etzel (Germany) for gas trading purposes.

Further information publicly available may be accessed at [6] which includes information on the Cavern Storage Etzel where Crystal is currently being commissioned.

The scope of the project relevant for this Initial Status Review is Functional Design and Basic Design and Detail Design.

2.1.3.4 Project 3

The purpose of the IOS Compressor Station Quarnstedt project is to increase the pressure of gas transported in the DEUDAN pipeline in south-north direction, in order to ensure that contractual delivery quantities and pressures are met at the hand-over point at the Danish border. The Compressor Station Quarnstedt is an intermediate compressor station and serves to compensate pressure drops along the pipeline in order to provide the required suction pressure at the downstream Compressor Station Ellund.

Further information publicly available may be accessed at:

- [7] including general information on the gas network expansion by Gasunie which Quarnstedt will be part of
- [8] and [9] including general information for public consultations in German language

The scope of the project relevant for this Initial Status Review is Functional Design and Basic Design.

2.1.3.5 Project 4

The purpose of the WAG Plus 600 project is to increase capacity of the existing West-Austria Gas Pipeline by 600,000 Nm^3/h to 1,800,000 Nm^3/h maximum capacity by looping and boosting.

Further information publicly available may be accessed at [10].

The scope of the project relevant for this Initial Status Review is Functional Design and Basic Design.

2.2 Scope of Review

2.2.1 Checklist for Interviews

A Checklist for support of the interviews has been prepared. The Checklist shall be an aid for giving structure to the separate interviews and later comparing the answers rather than a strict protocol to be fulfilled. The Checklist has been prepared considering four aspects which have been found helpful in aligning the guidelines of the new approach with the system engineering work performed in EC:

- Elements of System Engineering
- Project Phase
- Levels of Intent Specification
- Elements of Using STAMP

Reference to the relevant chapter of Engineering a Safer World is also provided.

Table 1 shows an example of Checklist questions and their relevance regarding the aspects considered. The Checklist is provided in **Error! Reference source not found.**. The next sub sections briefly list the elements of the aspects considered.

Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question
Management	All	Level 0	Implementing a safety control structure	13.2.6	Is there a group in EC responsible for safety in the projects?
Development	Functional Design, Basic Design	Level 1	Generating system-level requirements	10.3.6	Are system-level requirements traceable back to the system goals and/or hazard analysis from where they have been generated?

Table 1: Example Checklist Questions

2.2.2 Elements of System Engineering

Based on Engineering a Safer World, Chapter 6, Figure 6.1:

- Engineering Development
- Operations
- Management

2.2.3 Project Phase

Based on terminology generally used in the industry:

- Feasibility (Facility Lifecycle Phase “Appraise”). Not in the scope of this thesis.
- Conceptual Design (Facility Lifecycle Phase “Select”)
- Functional Design (Facility Lifecycle Phase “Select”)
- Basic Design (Facility Lifecycle Phase “Define”)
- Detail Design (Facility Lifecycle Phase “Execute”). Not in the scope of this thesis.
- Construction and Commissioning (Facility Lifecycle Phase “Execute”). Not in the scope of this thesis.
- Operation (Facility Lifecycle Phase “Operate”). Not in the scope of this thesis.

2.2.4 Levels of Intent Specification

Based on Engineering a Safer World, Chapter 10, Figure 10.1 and Figure 10.2:

- Level 0: Program Management, Management View (Project management plans, status information, safety plan, etc.)
- Level 1: System Purpose, Customer View (System goals, high-level requirements, design constraints, limitations)
- Level 2: System Design Principles, System Engineering View (Logic principles, control laws, functional decomposition and allocation)
- Level 3: System Architecture, Interface between System and Component Engineers (Blackbox functional models, interface specifications)
- Level 4: Design Representation (Component Designer View). Not in the scope of this thesis.
- Level 5: Physical Representation (Component Implementer View). Not in the scope of this thesis.
- Level 6: System Operations (Operations View). Not in the scope of this thesis.

2.2.5 Elements of Using STAMP in System Engineering

According to outline of Engineering a Safer World, Chapter 10 with a selection of Management elements and interface elements to Operations as illustrated in Figure 5:

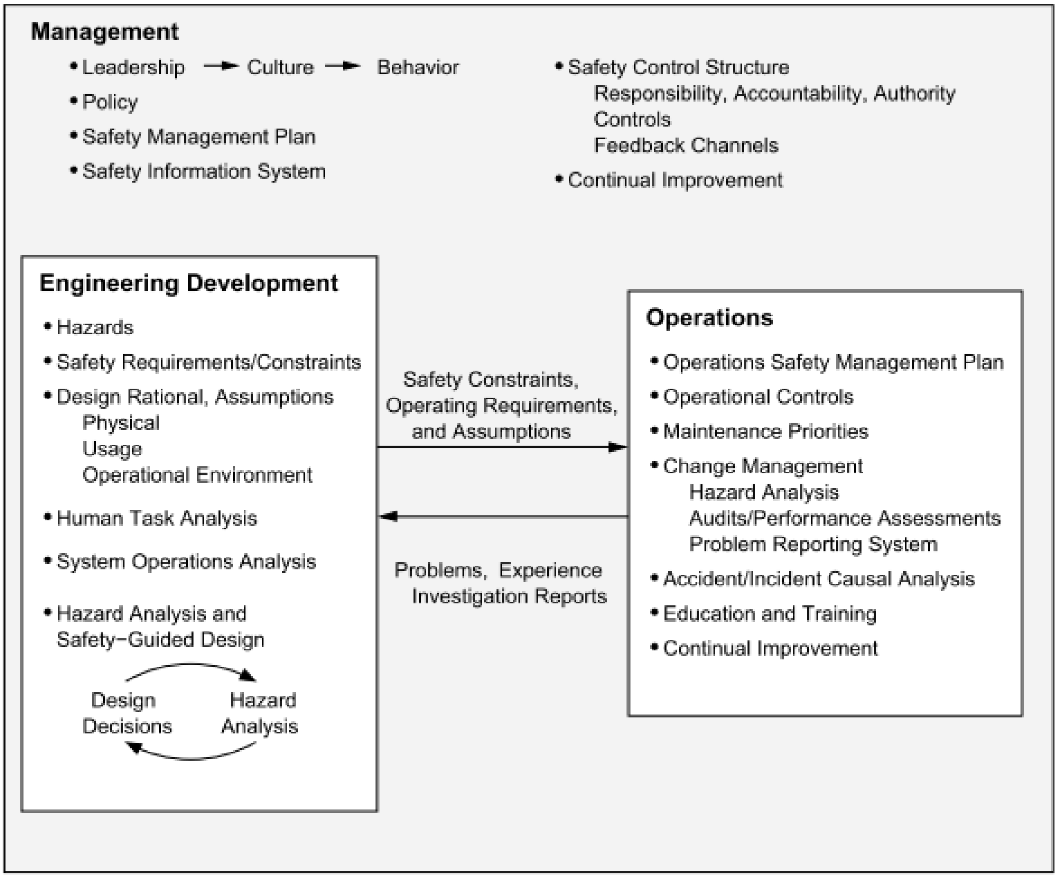

Management
• Leadership → Culture → Behavior
• Policy
• Safety Management Plan
• Safety Information System
• Safety Control Structure
Responsibility, Accountability, Authority
Controls
Feedback Channels
• Continual Improvement
Engineering Development
• Hazards
• Safety Requirements/Constraints
• Design Rational, Assumptions
Physical
Usage
Operational Environment
• Human Task Analysis
• System Operations Analysis
• Hazard Analysis and Safety–Guided Design
Design Decisions
Hazard Analysis
Safety Constraints, Operating Requirements, and Assumptions
Problems, Experience Investigation Reports
Operations
• Operations Safety Management Plan
• Operational Controls
• Maintenance Priorities
• Change Management
Hazard Analysis
Audits/Performance Assessments
Problem Reporting System
• Accident/Incident Causal Analysis
• Education and Training
• Continual Improvement

Figure 5: The Components of a System Safety Engineering Process based on STAMP [1]

- Establishing the Goals of the System
- Defining Accidents
- Identifying System Hazards
- Integrating Safety into Architecture Selection and System Trade Studies
- Documenting Environmental Assumptions
- Generating System-Level Requirements
- Identifying High-Level Design and Safety Constraints
- Performing System Design and Analysis
- Documenting System Limitations
- Considering relevant Operations Experience in the Development
- Delivering Safety Requirements and Constraints to Operations
- Providing Leadership for Safety Matters
- Implementing a Safety Policy
- Implementing a Safety Management Plan
- Implementing a Safety Control Structure
- Implementing a Safety Information System

Some STAMP elements have been excluded from the scope of the review and analysis because it has been considered that the other elements of the approach have a higher priority for implementation. These should be addressed once the results of this thesis have been implemented in EC:

- Continual Improvement (in Management)
- Human Task Analysis (in Engineering Development)
- Operations

2.3 Results of Review

The results of the review are provided in **Error! Reference source not found.** which contains a MS Excel file with all questions and all answers provided by the different interviewees. The analysis of the results is performed in the next chapter 3 for every step/ element reviewed.

3 Application of STAMP to Integration of Safety into System Engineering

This chapter describes the analysis of (i) Current EC practice, (ii) Feasibility of STAMP implementation for integration of safety into EC's system engineering process, (iii) Example of how the new techniques can be applied to a real project and (iv) Definition of high-level guidelines for implementation in EC. The requirements are then considered in the definition of an action plan for implementation of STAMP into EC's system engineering process in the next chapter.

3.1 Definition of Safety

Safety is defined in Engineering a Safer World as freedom from accidents (or loss events). This is a holistic definition which implies that any type of loss event impacts on safety. The Oil & Gas industry uses a more limited definition of safety the common understanding of which could be articulated as the absence of fatalities and injuries. Some operators do extend the definition of safety to HSE (Health, Safety and Security, and Environment protection). Some also like to consider impacts on Assets, Productivity and Reputation in the scope of HSE.

The analysis below is developed based on the limited definition of safety as absence of fatalities and injuries during system operation. Safety-related is defined herein as something which might influence safety, i.e. project activity which might influence the absence (or presence) of fatalities and injuries during system operation.

However it is observed that the potential of the new techniques goes beyond this limited definition. This might be the subject of further study (i.e. engineering to avoid any identified project or system losses).

3.2 Analysis of Elements of Using STAMP

3.2.1 Steps

Leveson defines the basic steps of applying STAMP to integrating safety into a system engineering process as follows (Outline Chapter 10 of Engineering a Safer World):

- Establishing the Goals of the System
- Defining Accidents
- Identifying System Hazards
- Integrating Safety into Architecture Selection and System Trade Studies
- Documenting Environmental Assumptions
- System-Level Requirements Generation
- Identifying High-Level Design and Safety Constraints
- System Design and Analysis
- Documenting System Limitations

These basic steps of engineering development together with a selection of management elements and interface elements to operations as illustrated in Figure 5 above:

- Considering relevant Operations Experience in the Development
- Delivering Safety Requirements and Constraints to Operations
- Providing Leadership for Safety Matters
- Implementing a Safety Policy
- Implementing a Safety Management Plan
- Implementing a Safety Control Structure
- Implementing a Safety Information System

have been analyzed in the following sections in terms of (i) Current EC practice, i.e. is EC if not formally, informally addressing that step as part of system engineering and if so how?, (ii) Feasibility of step implementation in EC and (positive) by-products, i.e. it is anticipated that by implementation of the new approach not only the safety of the engineered systems will be improved, but also the quality of the engineering work delivered (e.g. traceability of decisions, documentation of often undocumented assumptions and limitations), (iii) Development of step for a Project Example, (iv) Definition of high-level guidelines for implementation of step in EC.

The following management elements have not been developed in the Project Example, however they are addressed in the Initial Status Review and analyzed for implementation:

- Providing Leadership for Safety Matters
- Implementing a Safety Policy
- Implementing a Safety Management Plan
- Implementing a Safety Control Structure
- Implementing a Safety Information System

3.2.2 Engineering Development

3.2.2.1 Establishing the Goals of the System

3.2.2.1.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 1 to 5. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting “Establishing the goals of the system” in column “Element of Using STAMP”.

Functional system goals are usually agreed between EC and the client and documented in the project contract. Functional system goals are articulated in quantitative form therefore in order to be easy to understand for all stakeholders. Typical functional system goals include:

- System Throughput
- Properties of fluids processed for defined operation scenarios (composition, pressure, temperature, etc.)
- System Availability
- System Lifetime

EC often has to provide a process guarantee on functional system goals as part of contracts.

Other project and system goals are not articulated that straightforward. Examples of such are:

- Design development shall comply with applicable regulations, norms and standards
- Technology and design shall be state of the art
- Design shall minimize environmental impact

Safety-related goals and design philosophies are generally either not agreed or not clearly articulated. Some operators do provide safety policies as part of contracts to which EC must adhere. The client’s own policy and culture as well as country where the project is to be implemented (national laws, risk perception) seem to be the main factors influencing if and how safety-related goals are defined.

Inherited constraints are not usually documented as such along with systems goals in the contracts. However, when EC inherits a design from another organization, the documentation must be considered and is usually also part of the contract. According to EC’s IMS, a Design Review shall be performed whenever EC inherits a design. The depth of this review is influenced by the budget assigned to the project (sometimes this Design Review is not paid by the client). This is however a critical step in contracts where a process guarantee is to be provided by EC. If inherited constraints are not identified during proposal preparation and contract negotiations, they are then identified in the Design Review process and documented in a Design Review report which after discussion with client usually flows into the Basis of Design for the project. Sometimes inherited constraints are revised in the course of the discussions with client because decisions taken previously are not adequate or not valid anymore (e.g. pipeline route and definition of locations).

It is a common case that EC has performed Feasibility and/or Concept Selection in a project and later is awarded with the Basic Design and FEED. Also having performed Basic Design and FEED sometimes clients decide to continue with Detail Design, Construction Supervision and Commissioning under EC's responsibility. In these cases the time gap between project phases seems to be the main factor determining how easily the project teams identify inherited constraints. This might be related to the quality of inherited documentation.

3.2.2.1.2Feasibility of Step Implementation in EC and By-Products

Establishing the functional goals of the system and clearly documenting them as part of contracts is currently practiced by EC and clients.

Non-functional goals are not always identified and clearly formulated. In general, it is recognized that a more clear definition of non-functional goals would aid in aligning EC and clients on the expectations. Furthermore, during the Initial Status Review it was recommended not only to specify non-functional goals, but to make design philosophies (related to those goals) part of contracts. If clients have developed design philosophies, this is normally the case. The problem arises when clients have never operated systems before (e.g. typical case of pipeline joint ventures created for the projects). In this case EC design philosophies should be used. The review also remarked that adequate design philosophies are not available (they are incomplete and/ or inconsistent between each other) and that design philosophies should be developed in EC. Knowledge seems to be located with experienced individuals, not documented.

Also, in the contracts where EC inherits a design, the review showed that documenting system goals is considered a sensible practice by all interviewees.

For these reasons it is considered necessary and feasible to implement this step as far as clients allow for it. Implementing this step first at a high-level, as proposed by Leveson, is not considered to be costly and/or complex, the positive by-products however being of benefit for a more effective and less costly design development. Going beyond high-level system goals definition and negotiating design philosophies for the cases where client does not provide them would first imply costs of standardization in EC. This investment would soon pay-off, as recognized by the review interviewees, and would aid dissemination of knowledge within the EC Group.

3.2.2.1.3Development of Step for the Project Example

The System Goals defined herein are considered as part of a Level 1 Intent Specification.

	System Goals for Project Example
G.1	*Transport and deliver oil products Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA from the Refinery Komsomolsk to tankers in Port De-Kastri.*
G.2	*Ensure quality of Oil Products to be delivered remains within specification.*
G.3	*Do not create unnecessary constraints to the tanker fleet operation.*
G.4	*Minimize the risk of losses to comply with high-level industry standards.*

Table 2: Example of System Goals defined for the Komsomolsk – De-Kastri Project

3.2.2.1.4Definition of High-Level Guidelines for Implementation of Step in EC

The aim should be first to introduce agreement of high-level system (functional and non-functional) goals as part of contract negotiations. Contract documentation should include very few but clear system goals, towards which the design is to be oriented.

Guidelines for agreement and clear documentation of high-level system goals as part of contract negotiations should be developed. The audience for this should be project managers for acquisition (i.e. the managers in charge of preparing proposals and negotiating with clients) as well as project managers and engineering managers (i.e. the managers in charge of executing the contracts).

If the process of agreeing and documenting high-level system goals is not successful (for example because the client has very rigid contract formats which for whatever reason cannot be amended), high-level system goals should still be documented in the Basis of Design.

If EC inherits a design then the high-level system goals should be accompanied in the Basis of Design by the inherited design constraints (analysed during the Design Review process).

The second stage of implementation should aim at agreement of more elaborated goals such as safety-related design philosophies, if possible, during contract negotiations. This means somehow rather early agreeing on safety-related Requirements and Safety Constraints before a project is started and making those agreements part of contracts. In the case that the client has detailed Safety Policies including safety-related design philosophies, then these shall be complied with and are part of contracts anyways. In case that the client does not have a Safety Policy and safety-related design philosophies (which is a frequent case), then for effective negotiations, EC should be prepared for proposing an adequate Safety Policy and safety-related design philosophy for the project. For that purpose a Safety Policy (a policy on designing systems for Safety, see 3.2.4.2 “Implementing a Safety Policy”) and safety-related design philosophies need to be developed.

Because the Oil & Gas industry is a domain with experience and an extensive body of knowledge, it is envisaged that the EC standard safety-related design philosophies to be developed shall be initially based on international good practice (analysis of available regulations, norms and standards). Once these EC standard safety-related design philosophies have been prepared, they could be further analysed for improvement by performing STPA Analysis.

3.2.2.2 Defining Accidents

3.2.2.2.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 6 to 15. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting “Defining accidents and unacceptable losses” in column “Element of Using STAMP”.

The understanding of what are accidents and losses varies from interviewee to interviewee, and as reported from client to client. Generally both Business Unit Directors and Project Managers believe that accidents are somehow already defined in the Oil & Gas industry body of knowledge. Fire and explosion events as well as spills seem to be the type of events everybody understands as accidents, but it is recognized that the range of losses may be wider. Usually the country where the project is to be implemented and its regulations determine what types of accidental events are indentified as such. When the clients have a developed HSE policy, as explained in 3.1 Definition of Safety, they might consider further impacts on Assets, Productivity and Reputation in the wider scope of HSE. A non-integrated approach between HSE policy (HSE or safety-related risk assessments) and Project Success policy (project management related risk assessments) has also been observed for clients with developed policies.

The Risk Matrix method seems to be the most widespread method for deciding on acceptability of losses. Project Managers interviewed referred to this method (specifically Safety Layer Matrix method or Calibrated Risk Graph method in IEC 61511-3 necessary for SIL Assessment) when agreeing with client about types of losses and acceptability (or rating) of those. However these had been agreed just for the purpose of performing the SIL Assessment, not from the beginning so that system design could be guided to avoid unacceptable losses. Business Unit Directors reported that unacceptable losses are, if not explicitly, implicitly defined in applicable regulations, norms and standards and that some clients do include Risk Criteria as part of contracts. Therefore it can be observed that accidents and unacceptable losses for a specific project are usually documented as part of risk assessments and in some cases as part of contracts when clients have a very clear idea of what is acceptable and what not.

It is interesting to remark that the majority of interviewees associate acceptability or unacceptability of a loss with the concept of risk (Risk Matrix method) which, according to classic definitions, implies considering the probability of the loss besides its severity.

3.2.2.2.2Feasibility of Step Implementation in EC and By-Products

As for the agreement of non-functional system goals (previous step 3.2.2.1 “Establishing the Goals of the System”) generally it is recognized that agreement on unacceptable losses should be performed as part of contract negotiations and if this is not possible the earliest in the project (e.g. as part of the kick off meeting).

It is observed that agreeing on system goals and agreeing on accidents and unacceptable losses is somehow related at a very high-level, as unacceptable losses are outcomes which the system should try not to bring about therefore somehow being goals too. So in other words it is about defining on a very high-level what the system should do (system goals) and what the system should not do (accidents and unacceptable losses).

Agreeing on how to avoid unacceptable losses has to do with the safety-related design philosophies mentioned in previous step 3.2.2.1 “Establishing the Goals of the System”. If these are available and the requirement to use them has been made part of the contracts, then this is addressed. If not, EC should propose philosophies. Again this shall overall aid in aligning EC and clients on the expectations.

For these reasons it is considered necessary and feasible to implement this step as far as clients allow for it. Again as in step 3.2.2.1 “Establishing the Goals of the System”, implementing this step first in a high-level, as proposed by Leveson, is not considered to be costly and/or complex, the positive by-products however being of benefit for a more effective and less costly design development. Going beyond high-level system goals definition and negotiating design philosophies for the cases where client does not provide them would first imply costs of standardization in EC. This investment would soon pay-off, as recognized by the review interviewees, and would aid dissemination of knowledge within the EC Group.

3.2.2.2.3Development of Step for the Project Example

The following losses have been defined and are all considered unacceptable so that design should try to avoid or control them.

	Unacceptable Losses for Project Example
A.1	*Oil Products Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA cannot be transported and delivered. [G.1]*
A.2	*Oil Product tankers' schedules disrupted. [G.3]* ***Rationale:*** *Even if overall the target yearly throughput is reached as per [G.1], individual tankers might have to wait for oil products during single operations, which might imply a disruption of the tanker schedule and might mean payment of demurrage costs.*
A.3	*Quality of Oil Products delivered deviates from specification. [G.2]*
A.4	*Workforce or other stakeholders' fatality or permanent disability. [G.4]*
A.5	*Damage to the environment. [G.4]* ***Assumption:*** *The environment is understood as the natural, industrial or social environment beyond the battery limits of the facilities and pipeline corridor (Right Of Way).*
A.6	*Damage to pipeline system assets. [G.1], [G.2], [G.3], [G.4]* ***Rationale:*** *Damage to the assets typically implies loss of production which depending on the magnitude of the loss may affect the target yearly throughput [G.1], the quality of the Oil Products transported [G.2] or the tankers schedule [G.3] too.*

Table 3: Example of Unacceptable Losses defined for the Komsomolsk – De-Kastri Project

3.2.2.2.4Definition of High-Level Guidelines for Implementation of Step in EC

The guidelines proposed for the previous step 3.2.2.1 "Establishing the Goals of the System" can be applied in the same fashion to this step so that in addition to the system goals (what the system should do) also unacceptable losses are defined (what the system should not do). It is considered convenient to derive unacceptable losses from the system goals.

In this thesis safety is defined as absence of fatalities and injuries during system operation. However in the Oil & Gas industry, as indicated in 3.1 "Definition of Safety" and as illustrated in Table 3, unacceptable losses might be defined beyond fatalities and injuries. For this reason, and in view again of the experience and extensive body of knowledge available, it is considered sensible to develop a typical set of unacceptable losses. This set should be put in the form of a Risk Matrix Criteria (as this seems to be the most widely used way of illustrating losses and their acceptability). However considering the opinion of some interviewees on the difficulty of understanding what likelihoods actually mean, instead of using hazard likelihood combined hazard severity, plausibility of events could be used. Manageability of hazards could also be considered, or a combination of both. These would be discussed with the clients that do not provide own Risk Criteria and included in contract and Basis of Design. This measure should be performed in a first stage of step implementation.

In a second stage of step implementation, again as described above, the objective would be to develop a safety-related design philosophy where unacceptable losses would be considered especially as part of STPA Analysis.

3.2.2.3 Identifying System Hazards

3.2.2.3.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 16 to 29. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting "Identifying system hazards" in column "Element of Using STAMP".

The review team believes unanimously that component failures can be or lead to hazards, but not necessarily. Most of the interviewees referred to failures in safety critical systems as potential hazards. Safety Instrumented Functions are usually foreseen in order to put the system in a fail-safe status, for example in the event of identification of failure in a gas detection system, affected units are isolated and depressurized and ventilation ducts closed. If an ESD System (Emergency Shutdown System) fails to isolate and depressurize the section where a hydrocarbon release or LOC (Loss Of Containment) has been identified, major fire and explosion events may develop.

When asked about identification of high-level System Hazards the review team has answered in two different ways (i) some have associated the question with performing HAZID and (ii) others have pointed that high-level System Hazards are only identified if issues are evident, not systematically. The second interpretation seems to be more related to the type of System Hazards to be identified as part of a Level 1 intent specification (see Figure 7). The next point 3.2.2.4 "Integrating Safety into Architecture Selection and System Trade Studies" elaborates more on this and the relation to Concept Selection.

HAZID is often performed in the Oil & Gas industry following a checklist. An example of the typical checklist used in EC in shown in Table 4. Another typical checklist is the one provided in ISO 17776 "Petroleum and natural gas industries —Offshore production installations— Guidelines on tools and techniques for hazard identification and risk assessment".

Hazard Type	Guideword	Expanders
External and Environmental Hazards		
Natural Hazards	Extreme Weather	Temperature extremes
		Waves
		Wind

Hazard Type	**Guideword**	**Expanders**
		Dust
		Flooding
		Sandstorms
		Ice
		Blizzards
		Lightning
	Seismic Activity	-
	Erosion	Ground slide
		Coastal
		Riverine
	Subsidence	Ground structure
		Foundations
		Reservoir depletion
Environmental Impact	Discharges to Air	Flaring
		Venting
		Fugitive emissions
		Energy efficiency
	Discharges to Water	Drainage
		Water quality
		Waste disposal options
	Discharges to Soil	Drainage
		Chemical spillage
		Waste disposal options
	Location and Layout	Previous land use
		Vulnerable fauna and flora
		Visual impact
		Local population
		Area minimisation
External and 3rd Party Hazards	Sabotage	Internal security threats
		External security threats
	Terrorist Activity	Riots
		Civil disturbance
		Strikes
		Military action
		Political unrest
	Third Party Activities	Farming
		Fishing
		Local industry
	Helicopter/Aircraft Crash	-
Facility Hazards		
Process Hazards	Process Releases – Unignited	Gas clouds
		Gas detection
		Emergency response
	Process Releases – Ignited	Fire
		Explosion
		Heat
		Smoke

Hazard Type	**Guideword**	**Expanders**
		Fire detection
		Emergency response
	Process Releases – Toxic	H2S detection
		Emergency response
	Flaring	Heat
		Ignition source
		Location
	Venting	Discharge to atmosphere
		Location
		Dispersion
	Draining	-
	Sampling	Operator error
Accommodation and non-process area hazards	Non Process Fires	Control rooms
		Accommodation
	Smoke Ingress	Ingress to safe areas
		HVAC shutdown
	Gas Ingress	Ingress to safe areas
		HVAC shutdown
	Stacking and Storage	-
Health Hazards		
Health Hazards	Disease Hazards	Endemic diseases
		Infection
		Contaminated water/food
		Social (e.g. HIV)
Working Environment	Physical	Drinking water
		Lighting
		Noise
	Temperature	Extreme hot/cold
		Ventilation
		Guarding
	Atmospheres	Exhaust fumes
		Confined spaces

Table 4: A HAZID Typical Checklist

It can be observed that Table 4 is large and that the hazard registers generated addressing the checklist will be fairly long. Leveson argues that lengthy hazard registers are often the result of addressing causal factors of hazards in the scope of System Hazard identification. Table 4 shows that this is the case in the typical HAZIDs performed by the Oil & Gas industry, as most of the rows are causal factors of events such as fires, explosions and spills.

The HAZID format along with an example of how standard hazards are analyzed in EC is provided in Table 5. As it can be observed, defined Accidents or Unacceptable Losses are not formally considered. Strictly speaking, the way HAZID is performed is rather a preliminary hazard analysis on the basis of a predefined hazards checklist. Therefore in essence it is not a hazard identification exercise, but a qualitative hazard analysis.

Hazard	**Hazardous Event**	**Potential Consequences**	**Existing Safeguards**	**Recommendations**
EXTERNAL AND ENVIRONMENTAL HAZARDS				
Natural Hazards - Extreme Weather - Low temperatures	Freezing of condensate in equipment; e.g. filter separator, condensate tank, drain system	Overpressure through plugged lines leading to LOC	Periodical inspection, automatic controlled drain system, double jacket tanks	Consider providing for electrical heat tracing system
	Carbon steel below -25C causing embrittlement of pipes	Material cracks leading to LOC		Material specification to be checked for extreme local conditions
FACILITY HAZARDS				
Process Hazards – Venting – Ignition Source	Ignition of vent	Fire and/ or explosion	Venting philosophy and venting calculations consider a safe location of the vent stack	Venting area shall be fenced

Table 5: A Typical HAZID format and example

When asking if defined Accidents and Unacceptable Losses are considered when identifying high-level hazards, most of the interviewees interpreted the question as if a risk analysis is performed (for example using the Risk Matrix method which implicitly accounts for typical losses, as described in the previous point 3.2.2.2 “Defining Accidents”).

Domain experts are always involved in any hazard identification or hazard analysis exercise in EC. As already mentioned above knowledge seems to be located with experienced individuals, rather than documented. The company is aware of this and therefore there is generally a culture of asking expert colleagues.

The review team believes that the industry has defined standard hazards which always should be addressed. Again at this point (i) some refer to the predefined hazard checklist used in HAZID as in Table 4, (ii) while others have reported standard high-level hazards are:

- Loss Of Containment (LOC)
- Fire and Explosion
- Spill

When performing HAZID, recommendations or actions can be issued (see Table 5). These can include requirements and design constraints, the level of those however often depending on the design maturity. If only high-level evident hazards are identified, then most probably generation of high-level requirements and design constraints will not be performed.

It is believed that industry and client standards include already high-level Requirements and Design Constraints which are considered in the preparation of safety-related design philosophies. As introduced in 3.2.2.1 "Establishing the Goals of the System", if the client does not have safety-related standards, then often there is a lot of discussions and time used for agreeing on safety-related design philosophies. For that reason it was again mentioned the need of developing standard safety-related design philosophies in EC. However it has also been recognised that while a standard is definitely helpful, it is not sufficient and a project specific approach for design philosophies is still needed (developed on the base of standards, but adapted to the project specific particularities with the aid of hazard analysis techniques).

3.2.2.3.2Feasibility of Step Implementation in EC and By-Products

High-level System Hazard identification should be performed. Standard high-level hazards are defined in the Oil & Gas industry, as listed above (i) Loss Of Containment (LOC), (ii) Fire and Explosion and (iii) Spill. Other high-level System Hazards (evident issues specific to the project of matter) can be easily identified together with clients for example as part of kick-off meetings.

Leveson suggests to first identify a small set of high-level System Hazards, usually less than a dozen. This is feasible and it is not considered costly or complex.

3.2.2.3.3Development of Step for the Project Example

For the Project example the following system hazards have been identified.

	System Hazards for Project Example
H.1	*Pipeline System Blockage. [A.1], [A.2]*
H.2	*Oil Products cannot be delivered when required by tankers. [A.2]*
H.3	*Quality of Oil Products deviates from specification. [A.3], [A.2]*
H.4	*Fire and/ or explosion events. [A.4], [A.5], [A.6]* **Rationale:** Loss of Containment and product release which ignites.
H.5	*Spill to the environment. [A.5]* **Rationale:** Loss of Containment and product release which does not ignite, but which may contaminate the environment.

Table 6: Example of System Hazards identified for the Komsomolsk – De-Kastri Project

From these system hazards the following high-level safety constraints can be derived.

	High-level Safety Constraints for Project Example
SC.1	*Pipeline System must not block. [H.1]*
SC.2	*Oil Products must be ready for delivery when required by tankers. [H.2]*
SC.3	*Quality of Oil Products must not deviate from specification. [H.3]*
SC.4	*Fire and explosion events must be prevented. [H.4]*
SC.5	*Spills to the environment must be prevented. [H.5]*

Table 7: Example of High-level Safety Constraints derived for the Komsomolsk – De-Kastri Project

Strictly speaking in the frame of this thesis, SC.1, SC.2, SC.3 and SC.5 should be considered high-level Design Constraints, while SC.4 would be the only Safety Constraint according to 3.1 “Definition of Safety”.

3.2.2.3.4Definition of High-Level Guidelines for Implementation of Step in EC

Besides the standard high-level hazards defined in the Oil & Gas industry:

- Loss Of Containment (LOC)
- Fire and Explosion
- Spill

other standard high-level System Hazards should be identified within the body of knowledge of the Oil & Gas industry for the different types of systems which EC is designing. For example, for offshore installations, collapse of platform (not as a consequence of fire and explosion) could be considered. Once these standard lists are prepared, they can be discussed for specific projects and a small list of high-level System Hazards on which the whole hazard control arrangements are based can be defined.

3.2.2.4 Integrating Safety into Architecture Selection and System Trade Studies

3.2.2.4.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 6 to 42. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting “Integrating safety into architecture selection and system trade studies” in column “Element of Using STAMP”.

When performing concept selection safety is not considered in a systematic way. There is no systematic high-level System Hazards identification performed, as described in the previous chapter 3.2.2.3 “Identifying System Hazards” and therefore there is also no refinement of those high-level system hazards for the different feasible options proposed as part of preliminary hazard analysis in concept selection. The review reported that safety issues are only considered when those are evident issues. Some interviewees explained that only evident issues can be considered because there is not enough design information at that stage for adequately taking safety into consideration in the decisions. This way safety is usually considered later in the design process. But for example in pipeline projects, location selection is an activity where safety issues can be evident and are usually taken into consideration, often driven by authority requirements (e.g. preliminary ESIA).

It was also reported that decisions in concept selection are driven by the following factors:

- Technical aspects, such as Throughput, Availability and Expandability
- Economic aspects, typically CAPEX and OPEX

Most of the interviewees understood a preliminary hazard analysis as a typical HAZID exercise. Some also mentioned HAZOP and QRA when thinking about preliminary hazard analysis; however all arguing that it is not possible to perform a sensible preliminary hazard analysis without a certain degree of design maturity. When asked about the timing for performing preliminary hazard analysis (mainly understood as HAZID), most of interviewees answered that it should be performed as soon as possible because the later the issues are identified in the design process, the more difficult it is to implement mitigation measures (design changes) in order to reduce risk.

The general opinion is that estimating hazards likelihood is not easy and that estimation is especially difficult if there is no design available. This appears to conflict with the also general opinion that preliminary hazard analysis should be performed as soon as possible in a project. Many interviewees refer to the use of leak frequencies for types of equipment and operating conditions as recorded in available databases such as OREDA and EGIG, but recognize as well that the industry practices data fine tuning to some extent in order to achieve acceptable results in probabilistic assessments. Some participants note however that working with probabilities provides a framework to develop a design rationale. Overall this shows that managers are not convinced about the validity of techniques available for checking the level of safety of a the design, but live with those techniques because they allow them to regulate and document discussions (i.e. they are somehow able to justify trade-offs in deciding which proposed mitigation measures are implemented and which not in the design process). The interviewees who were asked their opinion about basing hazards likelihood estimations in historical data argued it is a good practice, especially for reliability studies, and that it provides good indication for estimates. The review team generally believes that estimating hazard severity is easier even if fire and explosion consequence simulation, which is performed aided by software, is complex and requires especial expertise. They also believe that estimating hazard severity makes sense.

The following table summarizes the general opinion on the preferred traditional hazard analysis techniques by managers interviewed.

Rank	**Hazard Analysis Technique**	**Advantages (according to interviewees answers)**	**Drawbacks (according to interviewees answers)**	**Interviewee recommends it?**
1	HAZOP	- Considers process hazards - Clear and systematic technique - No need special software	- Team effort, organizational difficulties - Time and cost intensive - Needs ready for approval PIDs and Operation Philosophy	Yes, EC standard

Rank	Hazard Analysis Technique	Advantages (according to interviewees answers)	Drawbacks (according to interviewees answers)	Interviewee recommends it?
2	HAZOP together with SIL	- Compact format (teams can be efficient analyzing SIFs) - Clear and systematic techniques - No need special software	- Team effort, organizational difficulties - Time and cost intensive - Needs ready for approval PIDs and Operation Philosophy	Yes
3	HAZID	- Simple - Does not need a very developed design - Considers all kinds of hazards - No need special software	- Team effort, organizational difficulties - Time and cost intensive	Yes
4	QRA	- Considers layouts - Provides good framework for decisions - Individual effort, organization easy	- Time and cost intensive - Need special software - Requires rather developed design - Lots of assumptions and data used	No
5	SIL alone	- Provides good framework for specification of SIFs equipment - No need special software	- Team effort, organizational difficulties - Time and cost intensive	No

Table 8: Traditional hazard analysis techniques ranking

3.2.2.4.2Feasibility of Step Implementation in EC and By-Products

The review generally reported that safety is only considered during Concept Selection if very evident issues are identified, or at a very high-level. Then when asked about preliminary hazard analysis, interviewees talked most of the time about HAZID which, as described above, is performed on the basis of a check-list leading to produce lengthy hazard registers. These hazard registers cannot be considered to contain only high-level System Hazards. Then HAZID as such is not usually performed during Concept Selection, but later when a certain design maturity has been reached. This shows that what is actually needed for the Concept Selection phase is a simple, but systematic way to compare options in view of identified high-level System Hazards (i.e. evident issues as articulated by the review). Once a pre-selection of options has been performed, usually in terms of feasibility and functionality, then performing a comparison of options for safety should not be too costly and/or complex. Even if ultimately the drivers for selection are CAPEX and OPEX and a less safe option might be selected, the exercise will trigger thinking why an option is considered safer than another, and that to some extent already leads to thinking about the controls necessary to mitigate the hazards. An example of this type of exercise is included in **Error! Reference source not found.** and introduced in the next point. Overall it is believed that this type of exercise will also contribute to deliver a better rationale on the concept selected.

3.2.2.4.3Development of Step for the Project Example

This step has not been developed for the Project Example “Oil Product Pipeline Komsomolsk – De-Kastri”, but for another project where the author had tried to introduce this step before. The reason why, as reported in the previous sections on current practice, is that safety is not systematically considered in the concept selection studies. During the concept selection phase of the “Oil Product Pipeline Komsomolsk – De-Kastri” three studies have been performed:

- Pipeline System Selection Study [11]
- Oil Product Logistic Transportation Model Study [12]
- Multiproduct Technology Study aiming to ensure Product Quality [13]

The following table maps the defined System Goals to the studies performed on which the concept selection decision is based.

Study performed for concept selection	**Related System Goal**
Pipeline System Selection Study [11]	**G.1** “*Transport and deliver oil products Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA from the Refinery Komsomolsk to tankers in Port De-Kastri.”*
Oil Product Logistic Transportation Model Study [12]	**G.1** “*Transport and deliver oil products Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA from the Refinery Komsomolsk to tankers in Port De-Kastri.”* **G.3** “*Do not create unnecessary constraints to the tanker fleet operation.”*
Multiproduct Technology Study aiming to ensure Product Quality [13]	**G.2** “*Ensure quality of Oil Products to be delivered remains within specification.”*

Table 9: Studies performed for concept selection of the Komsomolsk – De-Kastri Project mapped to defined System Goals

None of these is explicitly concerned with (i) ensuring safety as defined in goal G.4 “*Minimize the risk of losses to comply with high-level industry standards”*–see Table 2– or (ii) avoiding defined losses A.4 “*Workforce or other stakeholders’ fatality or permanent disability”*–see Table 3–.

The project in which a simple trade analysis considering safety was performed is “FEED & PMC for Installation of a Single Point Mooring (SPM) in Bangladesh”, also known as “Kutubdia-Chittagong pipeline system”. **Error! Reference source not found.** includes the complete exercise performed.

The parameter “Health, Safety & Security” in the trade analysis was defined as the ability of a design option (a certain system configuration proposed) to ensure the health, safety and security of stakeholders in normal conditions or under hazardous loads of any kind. The “Health, Safety & Security” had to be evaluated using a range of numeric values from 1 to 5, so that 1 should be assigned to an inherently more hazardous solution and 5 to an inherently safer/more secure solution. The risks identified concerning “Health, Safety & Security” were the following (these can be interpreted as system hazards which could have been identified as part of STAMP step 3.2.2.3 “Identifying System Hazards”):

- SPM unloading solution and related pipes with high number of interconnections more prone to LOC potentially leading to incidents and loss of operation.
- Marine soil settlement and sedimentation might lead to increase of SPM chain tension eventually reaching maximum tension and failing possibly leading to incidents and loss of operation.
- Onshore part of facility is exposed to natural hazards (earthquake, soil liquefaction, hurricane, storms, landslide, and high tide) potentially leading to incidents and loss of operation. Specific Geo/Seismic hazards assessment will be performed by local environmental partner.
- Offshore part of facility is exposed to natural hazards (earthquake, soil liquefaction, hurricane and storms) potentially leading to incidents and loss of operation. Specific Geo/Seismic hazards assessment will be performed by local environmental partner.
- Pump Station might be exposed to flooding, if not located on a hill, potentially leading to incidents and loss of operation.
- Vulnerable population along onshore routes potentially exposed to fire and/or explosion in the event of LOC leading to major incidents and major loss of operation.
- Vandalism on onshore parts of facility causing LOC developing in fire and/or explosion leading to major incidents and major loss of operation.

These hazards were evaluated for the different options proposed obtaining the following ranking in terms of “Health, Safety & Security”:

Rank	**Option**	**Points awarded for “Health, Safety & Security”**
1	Option 1 – Onshore Pump Station with Onshore Pipeline	3
1	Option 10 – Onshore Pump Station on Kutubdia Island with Offshore Pipeline	3
2	Option 4a – Onshore Pump Station and Tank Farm with Offshore Pipeline	2
2	Option 7 – Onshore Pump Station with Offshore Pipeline	2

Rank	Option	Points awarded for "Health, Safety & Security"
2	Option 11 – Onshore Pump Station and Tank Farm on Kutubdia Island with Offshore Pipeline	2
3	Option 2 – Onshore Pump Station and Tank Farm with Onshore Pipeline	1

Table 10: Options Ranking "Health, Safety & Security" for "FEED & PMC for Installation of a Single Point Mooring (SPM) in Bangladesh"

This ranking was considered together with the evaluation of other risks related to Design Maturity, Operability, Reliability, Maintainability, Adaptability, impact to Environment, impact to Society and Execution Schedule.

This is only an excerpt of the brief analysis performed. **Error! Reference source not found.** includes the complete exercise for illustration of what can be done quite simply.

3.2.2.4.4Definition of High-Level Guidelines for Implementation of Step in EC

After identifying a small set of evident high-level System Hazards, as described in 3.2.2.3 Identifying System Hazards, a comparison of pre-selected options should be performed. This can be performed as a workshop. Different approaches might be used for that. One approach could be as in the example provided in **Error! Reference source not found.**, but another could be a more typical preliminary hazard analysis evaluating identified hazards for the different options, instead of awarding points as in the relative ranking method, using a Risk Matrix, as explained in 3.2.2.2. The first approach could be more easily implemented than the second one, since the Risk Matrix approach implies first agreeing on which outcomes are acceptable or not.

3.2.2.5 Documenting Environmental Assumptions

3.2.2.5.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 43 to 47. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting "Documenting environmental assumptions" in column "Element of Using STAMP".

Assumptions are understood by the review team as either (i) data which the client has not provided or is not able to confirm or as (ii) data which is not available because a design has not sufficiently progressed but designers have to estimate in order to perform their portion of design. A typical example of (ii) is piping and layout designers making assumptions about dimensions of equipment, when information about those dimensions is not available because equipment has not been yet procured. The way piping is designed is a very significant factor influencing pressure drop in a facility, which is often a functional system goal (i.e. facility outlet pressure has to be ensured) for which EC has to provide a process guarantee as part of contracts.

Assumptions are usually recognised as such and documented in the Basis of Design. However the paragraphs of a typical Basis of Design do not always explicitly indicate that certain data are assumptions (as opposed to an intent specification approach where assumptions are flagged as such and the parts of the design which use them can be traced, this way if assumptions change it is easy to find where impacts of changes have to be checked).

Even if assumptions are generally recognised as such and documented, over time designers forget that those pieces of data were assumptions and that they may not hold anymore, therefore needing to be verified. This is of special relevance progressing from one project phase (e.g. Basic Design) to the next (e.g. Detail Design), and considering that sometimes the time gap between them is large (e.g. years). Other assumptions such as the ones of the example used for piping design do not find their way in the Basis of Design and there is no formal documentation unless the designer decides to prepare a list by him(her)self. For these cases design review meetings such as 3D walkthroughs are performed. While the value of these review sessions is not questioned, it is believed that documenting usually undocumented assumptions would improve between others the efficiency of the review sessions.

Documentation of assumptions in the hazard analysis process is poor and very dependent on the hazard analysis team composition. If the hazard analysis team includes only project team members, then assumptions might go undocumented because those are clear for the project team members. But if the team includes individuals external to the project, then assumptions would probably get documented. Clients are sometimes afraid of providing rationale about findings and recommendations (while this might be country or culture related, the author has experienced this behaviour in Europe as well as in China). A very typical example is the assumptions made during a HAZOP session in Basic Design. The recommendations on operating procedures will only hold later when handing over to operations, if the assumptions hold too.

The review team agreed that the importance of assumptions is fundamental for ensuring safe operation.

3.2.2.5.2Feasibility of Step Implementation in EC and By-Products

The review team reported unanimously that assumptions should be identified and documented as early as possible in projects and verified and updated later on when more information is available. In order to ensure this, systematic documentation of assumptions needs to be performed.

While some projects are more formal than others in the management of data and assumptions, it cannot be stated that there is a system in place for management of assumptions. This relies on the fact that the Basis of Design is seen as a document more than as a database, and since Basis of Design for different projects are prepared by different individuals, what gets documented and how it gets documented differs from project to project. Currently there are discussions in EC about the purpose, content, frequency of revision and a possible standardization on preparation of Basis of Design. The opinion of the author is that the Basis of Design should be treated as an intent specification (see Figure 5 and Figure 6) which might be revised in all its levels as the design work progresses at defined project stages (e.g. Gate Reviews).

For these reasons it is considered necessary and feasible to implement this step. Again implementation of this step is expected to not only improve the safety of the engineered systems, but also the efficiency of engineering management activities and the quality of the engineering work delivered.

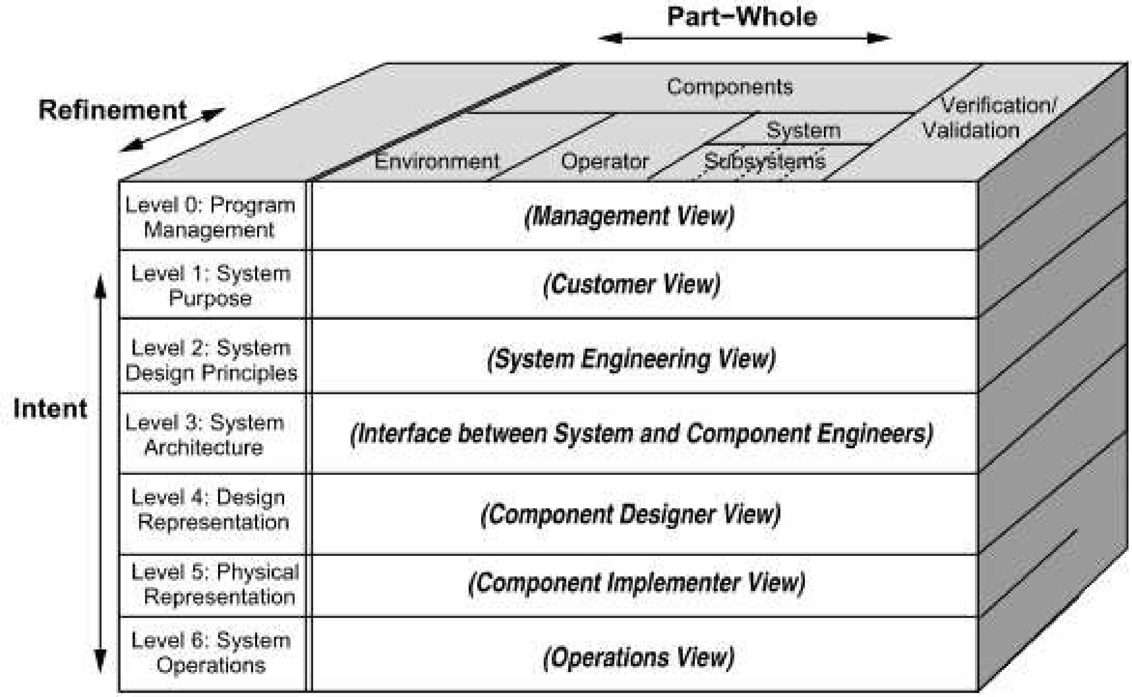
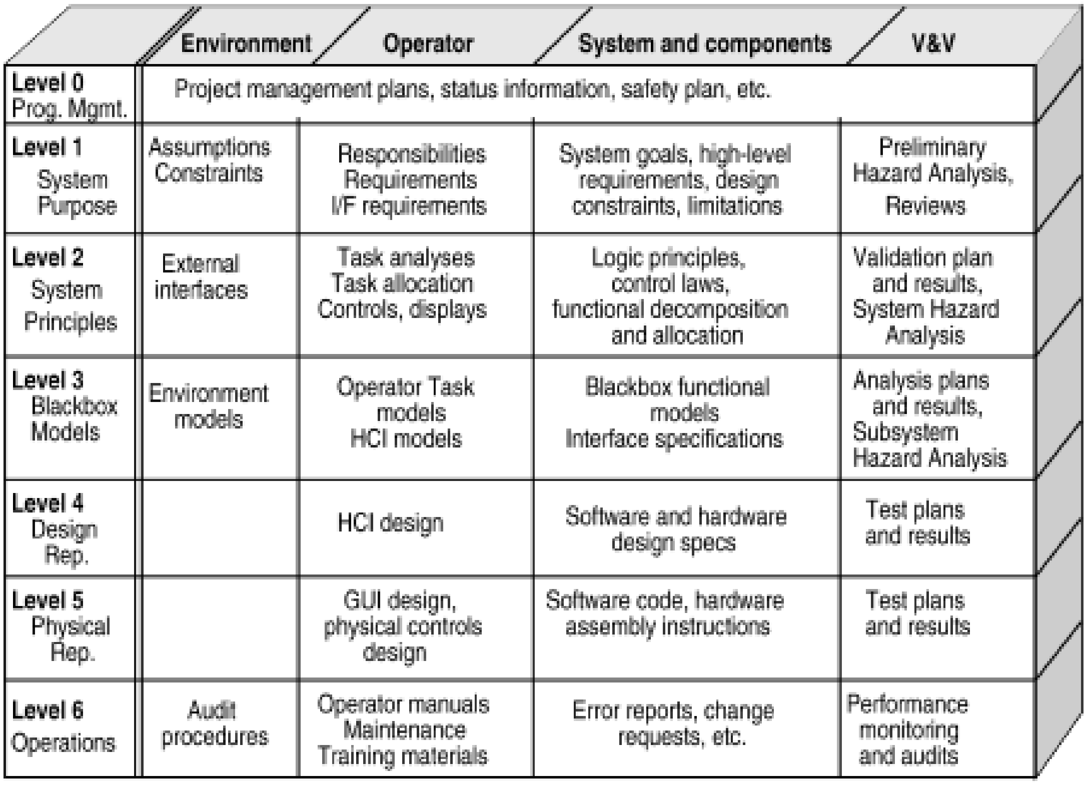

Part–Whole
Refinement
Components
Environment
Operator
System
Subsystems
Verification/ Validation
Intent
Level 0: Program Management
(Management View)
Level 1: System Purpose
(Customer View)
Level 2: System Design Principles
(System Engineering View)
Level 3: System Architecture
(Interface between System and Component Engineers)
Level 4: Design Representation
(Component Designer View)
Level 5: Physical Representation
(Component Implementer View)
Level 6: System Operations
(Operations View)

Figure 6: The Structure of an Intent Specification [1]



	Environment	Operator	System and components	V&V
Level 0 Prog. Mgmt.	Project management plans, status information, safety plan, etc.			
Level 1 System Purpose	Assumptions Constraints	Responsibilities Requirements I/F requirements	System goals, high-level requirements, design constraints, limitations	Preliminary Hazard Analysis, Reviews
Level 2 System Principles	External interfaces	Task analyses Task allocation Controls, displays	Logic principles, control laws, functional decomposition and allocation	Validation plan and results, System Hazard Analysis
Level 3 Blackbox Models	Environment models	Operator Task models HCI models	Blackbox functional models Interface specifications	Analysis plans and results, Subsystem Hazard Analysis
Level 4 Design Rep.		HCI design	Software and hardware design specs	Test plans and results
Level 5 Physical Rep.		GUI design, physical controls design	Software code, hardware assembly instructions	Test plans and results
Level 6 Operations	Audit procedures	Operator manuals Maintenance Training materials	Error reports, change requests, etc.	Performance monitoring and audits

Figure 7: An Example of the Information in an Intent Specification [1]

3.2.2.5.3Development of Step for the Project Example

A so-called list of input data was prepared by the Project. This list contains besides confirmed data also assumptions. The list of input data was later transposed to a Basis of Design [14]. The table below shows some examples of the assumptions part of that Basis of Design.

	Some Assumptions for Project Example
EA.1	*There are no permafrost areas along the pipeline route.*
EA.2	*Burial depth to the center line of pipe is 1.5 m.*
EA.3	*Inlet fluid pressures at the battery limit with the Refinery Komsomolsk are Diesel 0.99 barg, Naphtha 1.01 barg and Jet A1 1.25 barg.*
EA.4	*Flashpoints of products received from the Refinery Komsomolsk are Diesel 67 deg C, Naphtha -25 deg C and Jet A1 38 deg C.*
EA.5	*Inlet fluid temperatures at the battery limit with the Refinery Komsomolsk are Diesel 5 deg C, Naphtha 5 deg C and Jet A1 5 deg C.*
EA.6	*System Operational Availability Factor is 93.20 %.*
EA.7	*Pump Efficiency is 85 %.*
EA.8	*Pumps' Mean Time Between Failures is 0.5 years.*
EA.9	*Maximum De-Kastri Port downtime due to bad weather conditions is 8 days.*
EA.10	*There is no fixed ice at De-Kastri Port during winter periods.*

Table 11: Examples of Assumptions identified for the Komsomolsk – De-Kastri Project [13], [14]

3.2.2.5.4Definition of High-Level Guidelines for Implementation of Step in EC

Overall the intent should be to handover a valid list of assumptions to operations at the end of the project Execution phase. EC should promote this practice through the different project phases where it is involved, not only if involved in Execution, but also starting from the Conceptual Design phase.

Basis of Design should document and flag assumptions as such. Different engineering and design disciplines are involved in preparing Basis of Design. The project engineering manager or sometimes project manager (in EC project managers are also engineering managers, depending on the size of the project) ensure consistency of inputs to Basis of Design by different engineering and design disciplines.

Engineering managers should request discipline leaders to list assumptions when they write their inputs to Basis of Design. A database format would be preferred as illustrated in Table 12. A project list of assumptions should be issued at least internally.

The list of assumptions should be reviewed during design review meetings of any kind and especially during Gate Review meetings.

ID	Assumption	Made by Discipline	To be Verified by Discipline	Directly Used in (part of design)	Impact of Changes To be Checked by Discipline	Date Last Check	Status [valid, not valid]
EA.1	*There are no permafrost areas along the pipeline route.*	System Engineering	Geology	Hydraulics	System Engineering	25.01.2012	valid
EA.2	*Burial depth to the center line of pipe is 1.5 m.*	System Engineering	Pipeline Engineering	Hydraulics, Hazard Analyses	System Engineering, Safety Engineering	25.01.2012	valid
EA.3	*Inlet fluid pressures at the battery limit with the Refinery Komsomolsk are Diesel 0.99 barg, Naphtha 1.01 barg and Jet A1 1.25 barg.*	System Engineering	EXTERNAL Refinery Komsomolsk	Hydraulics	System Engineering	25.01.2012	valid
EA.4	*Flashpoints of products received from the Refinery Komsomolsk are Diesel 67 deg C, Naphtha 44 deg C and Jet A1 38 deg C.*	System Engineering	EXTERNAL Refinery Komsomolsk	Hydraulics, Hazard Analyses	System Engineering, Safety Engineering	25.01.2012	valid
EA.5	*Inlet fluid temperatures at the battery limit with the Refinery Komsomolsk are Diesel 5 deg C, Naphtha 5 deg C and Jet A1 5 deg C.*	System Engineering	EXTERNAL Refinery Komsomolsk	Hydraulics	System Engineering	25.01.2012	valid
EA.6	*System Operational Availability Factor is 93.20 %.*	System Engineering	EXTERNAL Refinery Komsomolsk	Hydraulics, Tank farm size optimization	System Engineering	25.01.2012	valid
EA.7	*Pump Efficiency 85 %.*	System Engineering	Mechanical	Hydraulics	System Engineering, Mechanical	25.01.2012	valid
EA.8	*Pumps' Mean Time Between Failures is 0.5 years.*	System Engineering	Mechanical	Tank farm size optimization	System Engineering, Mechanical	25.01.2012	valid
EA.9	*Maximum De-Kastri Port downtime due to bad weather conditions is 8 days.*	System Engineering	EXTERNAL Port De-Kastri	Tank farm size optimization	System Engineering	25.01.2012	valid
EA.10	*There is no fixed ice at De-Kastri Port during winter periods.*	System Engineering	EXTERNAL Port De-Kastri	Tank farm size optimization	System Engineering	25.01.2012	valid

Table 12: Example of Assumptions List format for the Komsomolsk – De-Kastri Project

Gate review meetings should include verification of assumptions and decision on what pieces of data remain as assumptions and which are revised as confirmed data for the next project phase.

This assumption management approach could be implemented right away.

Documenting assumptions during hazard analysis could also be implemented right away, at least for the hazard analyses where EC has a chairman role.

3.2.2.6 Generating System-Level Requirements

3.2.2.6.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 48 to 52. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting “Generating system-level requirements” in column “Element of Using STAMP”.

The review team understands system-level requirements are requirements to the system to be engineered as a whole, and recognize that goals are usually more abstractly articulated than Requirements, which are usually measurable.

System-level requirements (safety-related and not safety-related) are generally documented in the Basis of Design. Sometimes contracts also include paragraphs with system-level requirements; in this case those requirements are transposed to the Basis of Design. Regarding safety-related requirements, some projects prepare a separate safety design philosophy, often including a certain level of detail from the first issue, which is gradually revised as the design progresses and new (safety-related) requirements are defined in the different hazard analyses performed.

Traceability of system-level requirements (safety-related and not safety-related) back to system goals and hazard analyses performed is generally not possible. The other way around (i.e. from goals and hazard analyses to requirements) is possible, however not straightforward. Sometimes the client has required preparing a so-called “Design Accidental Loads Specification”, which is a set of safety-related requirements, usually including definition of heat and overpressure loads which structures should withstand. In this case, reference to a consequence analysis or QRA performed before is provided and traceability can be ensured. But this is not the common practice in EC.

Interviewees report that recommendations and actions (safety-related requirements) issued in hazard analyses are followed-up for implementation.

3.2.2.6.2Feasibility of Step Implementation in EC and By-Products

Again the Basis of Design is the document where requirements are documented. However, as already indicated in the previous points, since Basis of Design for different projects are prepared by different individuals, what gets documented and how it gets documented differs from project to project. So currently there is no consolidated approach to developing the rationale about design decisions, as opposed to the frame an intent specification would provide.

As reported above, currently there are discussions in EC about the purpose, content, frequency of revision and a possible standardization on preparation of Basis of Design. This standardization process could be guided by the principles of an intent specification.

This way not only the safety of the engineered systems could be improved, but also the efficiency of engineering management activities and the quality of the engineering work delivered.

3.2.2.6.3Development of Step for the Project Example

The main system goal is G.1 *"Transport and deliver oil products Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA from the Refinery Komsomolsk to tankers in Port De-Kastri"*.

Some of the system-level requirements (not safety-related) documented in the Project Basis of Design [14] are listed in Table 13.

	Some System-Level Requirements for Project Example
1.1	*The pipeline system shall transport and deliver 5.7 MTA of oil products: Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA.*
1.2	*The pipeline system lifetime shall be 33 years.*
1.3	*The pipeline system shall transport the oil products by batching (consecutive pumping) using the direct contact method (without batch separation means).*
1.4	*The pipeline system operation mode shall be 365 days, 24 hours.*
1.5	*The pipeline system planned maintenance periods shall be every 3 years: 15 days of shutdown per year for 2 years and 45 days of shutdown per year for 1 year.*

Table 13: Examples of System-Level Requirements identified for the Komsomolsk – De-Kastri Project [14], [16]

3.2.2.6.4Definition of High-Level Guidelines for Implementation of Step in EC

In general, standard design philosophies (safety-related and not safety-related) should be developed. These philosophies should first be developed considering the body of knowledge of the Oil & Gas industry, and afterwards improved by applying STPA. Standard philosophies should be considered when preparing Basis of Design and performing hazard analyses, but should be adapted to the particularities of specific projects.

3.2.2.7 Identifying High-Level Design and Safety Constraints

3.2.2.7.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 53 to 58. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting "Identifying high-level design and safety constraints" in column "Element of Using STAMP".

High-level design constraints (safety-related and not safety-related), as described above for system-level requirements, are generally documented in the Basis of Design. Sometimes contracts also include related paragraphs which are transposed to the Basis of Design. Regarding safety-related design constraints, some projects prepare a separate safety design philosophy, often including a certain level of detail from the first issue, which is gradually revised as the design progresses and new (safety-related) design constraints are defined in the different hazard analyses performed.

Traceability of design constraints back to hazard analyses performed is generally not possible. The other way around is possible, however not straightforward. Interviewees report that recommendations and actions (safety-related design constraints) issued in hazard analyses are followed-up for implementation. However following how the design constraints have been used in related decisions and to which design features relate is generally not straightforward.

Conflicts between the different high-level design constraints generated are solved on a case by case basis. Some interviewees pointed that the fact of not having a developed and comprehensive Safety Policy with the aim of designing systems for safety does not help solving conflicts and contributes to costly internal and external discussions where finding consensus is difficult because there is no basis on which to argue (see 3.2.4.2 “Implementing a Safety Policy” below). A participant reported that in the organization where he previously worked, the figures of “Technical Authority” for the different disciplines and “Chief Engineer” were established in order to deal with solving conflicts. For example, if two technical authorities (e.g. process and safety) could not find consensus, then the issue was forwarded to the “Chief Engineer”. He remarked however, that most of the times issues didn’t need to get the attention of these authorities because there were design philosophies and policies regulating those.

Basis of Design differs from project to project, as repeatedly remarked in the previous points, but generally it can be stated that the level of detail of the design philosophies documented there varies (i.e. some parts list high-level requirements and constraints, while other parts already define design features to be implemented from the very first issue of the document). Revision of Basis of Design is not performed as design decisions progress.

3.2.2.7.2Feasibility of Step Implementation in EC and By-Products

As already suggested above, currently there are discussions in EC about the purpose, content, frequency of revision and a possible standardization on preparation of Basis of Design. This standardization process could be guided by the principles of an intent specification. This way not only the safety of the engineered systems could be improved, but also the efficiency of engineering management activities and the quality of the engineering work delivered.

3.2.2.7.3Development of Step for the Project Example

High-level safety constraints have been derived from the identified system hazards in Table 7 of 3.2.2.3 “Identifying System Hazards”:

- SC.1: *Pipeline System must not block. [H.1]*
- SC.2: *Oil Products must be ready for delivery when required by tankers. [H.2]*
- SC.3: *Quality of Oil Products must not deviate from specification. [H.3]*
- SC.4: *Fire and explosion events must be prevented. [H.4]*
- SC.5: *Spills to the environment must be prevented. [H.5]*

As remarked above, strictly speaking in the frame of this thesis, SC.1, SC.2, SC.3 and SC.5 should be considered high-level design constraints, while SC.4 would be the only safety constraint according to 3.1 "Definition of Safety".

SC.1 and SC.2 can be refined considering the analysis performed in the Oil Product Logistic Transportation Model Study [12], for example:

- SC.1: *Pipeline System must not block. [H.1]*
    - *Sufficient equipment spare units must be provided to ensure continuation of system operation in the event of equipment breakdown.*
    - *Sufficient Oil Product stock in Head Tank Farm must be available to ensure continuation of system operation in the event of Refinery supply stoppage.*
- SC.2: *Oil Products must be ready for delivery when required by tankers. [H.2]*
    - *Stock available in the De-Kastri Tank Farm must be sufficient to fulfill demand of tankers waiting at the Port*

SC.3 can be refined considering the analysis performed in the Multiproduct Technology Study aiming to ensure Product Quality [13], for example:

- SC.3: *Quality of Oil Products must not deviate from specification. [H.3]*
    - *Jet A1 Fuel must be transported through pipeline section II between batches of Diesel Fuel only.*
    - *Naphtha must be transported between batches of Diesel Fuel only*
    - *Contaminate Mix of Jet A1 Fuel and Diesel Fuel must not be re-injected to Jet A1 Fuel.*

These refined constraints have been listed below in Table 15 and Table 16 as high-level operation and design constraints. It is however observed that the refinement of these constraints, originally derived as safety constraints from system goals and unacceptable losses, and overall the rationale to arrive at that refinement could probably be improved applying STPA techniques.

SC.4 and SC.5 have not been refined during the Conceptual Design work, as remarked above in 3.2.2.4 "Integrating Safety into Architecture Selection and System Trade Studies". SC.4 will be addressed (refined) in the next point 3.2.2.8 "Performing System Design and Analysis".

Table 14 lists examples of inherited constraints from the previous Investment Justification work which EC has to adhere to while developing the design of the Komsomolsk – De-Kastri Project.

	Some Inherited Design Constraints for Project Example	**Type**
C.1	*Investment costs must not exceed estimated CAPEX as in previous Investment Justification work.*	*Economic*
C.2	*System Operation Costs must not exceed estimated OPEX as in previous Investment Justification work.*	*Economic*

	Some Inherited Design Constraints for Project Example	**Type**
C.3	*Design must comply with VNTP-3-90 "Technological Engineering standards for branched pipelines; Instructions for technology of batch pumping of oil products through main oil product pipelines".* **Rationale:** Design must comply with applicable Russian regulations. If the optimized design by EC proposes deviations, then these need to be negotiated with the relevant authorities.	*Norms and Standards*
C.4	*The pipeline system must follow the corridor of the existing pipelines "Okha – Komsomolsk-on-Amur" and "Sakhalin – Vladivostok".*	*Route*
C.5	*Pipeline KP 0 must be located at Komsomolsk Metering Station (KMS)*	*Route*
C.6	*The pipeline system sections I and III must provide dedicated lines for the different oil products. (↓2.1, 2.2, 2.3, 2.5, 2.6, 2.7)*	*Design*
C.7	*The pipeline system must provide for a Tank Farm at the start of the pipeline section II for coping with fluctuations of supply.*	*Design*
C.8	*Head Tank Farm must be located at KP 4.133.*	*Route*
C.9	*The pipeline system must provide for a Tank Farm at the end of the pipeline section II for coping with fluctuations of demand.*	*Design*
C.10	*De-Kastri Tank Farm must be located at KP 330.*	*Route*
C.11	*De-Kastri Loading Point (DLP) must be located at KP 333.285.*	*Route*
C.12	*If an Intermediate Pump Station is required in pipeline section II, then a power generation plant with gas turbine must be provided.*	*Design*
C.13	*Pumps' drivers must be electrical motors for each pump station.*	*Design*
C.14	*Loading point type must be Arctic Loading Tower.*	*Design*
C.15	*Loading point must provide for 2 berths.*	*Design*

Table 14: Examples of Inherited Design Constraints identified for the Komsomolsk – De-Kastri Project [14]

Table 15 lists examples of operation constraints which have been identified for the design of the Komsomolsk – De-Kastri Project while performing trade studies.

	Some High-level Operation Constraints for Project Example
OP.1	*Jet A1 Fuel must be transported through pipeline section II between batches of Diesel Fuel only. (→Multiproduct Technology Study [13])*
OP.2	*Naphtha must be transported through pipeline section II between batches of Diesel Fuel only. (→Multiproduct Technology Study [13])*

	Some High-level Operation Constraints for Project Example
OP.3	*Contaminate Mix of Jet A1 Fuel and Diesel Fuel must not be re-injected to Jet A1 Fuel. (→Multiproduct Technology Study [13])*
OP.4	*When tankers are waiting at the anchorage in Port De-Kastri, priority must be FIFO (First In First Out). (→Oil Product Transportation Study [12])*
OP.5	*A tanker must not be able to leave the berth while another tanker is approaching the berth. (→Oil Product Transportation Study [12])*
OP.6	*Pipeline Maximum Batch Size for oil products must be equal to the largest tanker size considered for that oil product: Diesel Fuel 105,000 m^3, Naphtha 66,000 m^3, Jet A1 Fuel 53,000 m^3. (→Oil Product Transportation Study [12])*
OP.7	*Tanker operations must be possible year-round. (→Oil Product Transportation Study [12])*
OP.8	*Tanker Port Turnaround time must not exceed 38 h in Spring-Summer period and 47 h in Fall-Winter period. (→Oil Product Transportation Study [12])*
OP.9	*Simultaneous loading of 2 tankers must be possible. (→Oil Product Transportation Study [12])*
OP.10	*Planned Maintenance activities of De-Kastri Loading Point must be scheduled so as not to interfere with tankers' loading schedule. (→Oil Product Transportation Study [12])*

Table 15: Examples of High-level Operation Constraints identified for the Komsomolsk – De-Kastri Project [12], [13], [14]

Table 16 lists examples of high-level design constraints which have been identified for the design of the Komsomolsk – De-Kastri Project while performing trade studies.

	Some High-level Design Constraints for Project Example
C.16	*Minimum Pipe Wall Thickness in pipeline section I and II must be 6 mm. (→Pipeline System Selection Study [11])*
C.17	*Sufficient equipment spare units must be provided to ensure continuation of system operation in the event of equipment breakdown. (→Oil Product Transportation Study [12])*
C.18	*Sufficient Oil Product stock in Head Tank Farm must be available to ensure continuation of system operation in the event of Refinery supply stoppage. (→Oil Product Transportation Study [12])*
C.19	*Stock available in the De-Kastri Tank Farm must be sufficient to fulfill demand of tankers waiting at the Port. (→Oil Product Transportation Study [12])*
C.20	*Individual Tank Sizes in Tank Farms must be equal for a single oil product. (→Oil Product Transportation Study [12])*

	Some High-level Design Constraints for Project Example
C.21	*Tankers must not wait more than 12 h after acceptance of Notice Of Readiness by Port De-Kastri. (→Oil Product Transportation Study [12])*
C.22	*Filling and emptying of individual Tanks in Tank Farms at the same time must not be possible. (→Oil Product Transportation Study [12])*
C.23	*Contamination of Jet A1 Fuel must not be allowed. (→Multiproduct Technology Study [13], ↓2.20)*
C.24	*Actual Oil Product Mix Zone Length must not be greater than Calculated Oil Product Mix Zone Length. (→Multiproduct Technology Study [13], ↓OP.16, L3)*
C.25	*Flash Point of delivered Jet A1 Fuel must not be lower than specified. (→Multiproduct Technology Study [13])*
C.26	*Freezing Point of delivered Jet A1 Fuel must not be lower than specified. (→Multiproduct Technology Study [13])*
C.27	*Sulphur Content of delivered Diesel Fuel must not be higher than specified. (→Multiproduct Technology Study [13])*
C.28	*Flash Point of delivered Diesel Fuel must not be lower than specified. (→Multiproduct Technology Study [13])*
C.29	*Naphtha delivered must not contain traces of water. (→Multiproduct Technology Study [13])*
C.30	*Boiling Point of Naphtha delivered must not be higher than specified. (→Multiproduct Technology Study [13])*

Table 16: Examples of High-level Design Constraints identified for the Komsomolsk – De-Kastri Project [11], [12], [13]

3.2.2.7.4Definition of High-Level Guidelines for Implementation of Step in EC

On the one hand, as already suggested above, standard design philosophies (safety-related and not safety-related) should be developed. These philosophies should first be developed considering the body of knowledge of the Oil & Gas industry, and afterwards improved by applying STPA. Standard philosophies should be considered when preparing Basis of Design and performing hazard analyses, but should be adapted to the particularities of specific projects. This implementation measure requires time and costs as indicated before, but will pay off relatively soon.

On the other hand, the findings and recommendations of studies normally performed by EC in the Conceptual Design phase which deliver lots of design constraints (e.g. (i) Pipeline System Selection Study [11], (ii) Oil Product Transportation Study [12] or (iii) Multiproduct Technology Study [13]) should be transposed into a Basis of Design (or revision of Basis of Design) following an intent specification approach. This implementation measure requires time and costs too, but could gradually be implemented for single studies (i.e. a chapter of Basis of Design) in different projects.

3.2.2.8 Performing System Design and Analysis

3.2.2.8.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 59 to 66. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting "System Design and Analysis (safety-driven design)" in column "Element of Using STAMP".

HAZID, HAZOP and SIL are performed as workshops. While these techniques are generally accepted, managers associate them with lengthy and costly sessions, and they believe if safety-related philosophies would be developed and followed, these activities would be reduced. QRA is usually performed only if the client requires it. The general impression is that it involves even more effort and cost than HAZID, HAZOP and SIL, especially because of the simulation software required to perform it. The opinion about the value of QRA is diverse. Some managers do not see an added value, arguing that the results of QRA are (mis)used to justify design decisions rather than to analyze the level of risk. Other managers do note that a probabilistic assessment helps in dealing with the ever controversial issue of acceptability providing a quantitative and therefore easy to understand frame. Table 8 above in 3.2.2.4 "Integrating Safety into Architecture Selection and System Trade Studies" shows an overview of the opinions about the hazard analysis techniques used by EC.

HAZOP recommendations (refined safety-design constraints) related to changes in PIDs, Cause and Effect Charts and Operation and Control Philosophy are usually followed up and implemented. If a SIL assessment is performed, the recommendations are also implemented and target SIL values are used in related specifications.

Hazard Analysis	**When performed?**
HAZID	As soon as PFDs 100%, Layouts 70%, PIDs 70%, Operation and Control Philosphy 70%
HAZOP	As soon as PFDs 100%, PIDs 100%, Operation and Control Philosphy 100%
SIL	As soon as PFDs 100%, PIDs 100%, Operation and Control Philosphy 100%
QRA	After HAZID or as soon as requirements for HAZID completed

Table 17: Timing when Hazard Analyses are performed in a project

HAZOP is the only hazard analysis technique which is always performed by EC when EC develops PIDs in projects.

Conflicts between the design principles are solved on a case by case basis and documented in minutes of meetings. This has also been explained above in 3.2.2.7 "Identifying High-Level Design and Safety Constraints" and below in 3.2.4.2 "Implementing a Safety Policy".

3.2.2.8.2Feasibility of Step Implementation in EC and By-Products

It is not considered practicable to depart from the traditional hazard analysis techniques in the short term since these techniques are very rooted in the Oil & Gas industry practice:

- HAZID
- HAZOP
- SIL
- QRA

However it is considered feasible for example to expand the scope of HAZID and HAZOP, including elements of STPA (e.g. introducing guidewords/ deviations on enforcement of safety constraints). This should be practicable, since these techniques seem to be the most widely accepted and their scope is defined, besides clients and standards, by the chairman.

3.2.2.8.3Development of Step for the Project Example

Although the initial scope of work of EC in this Project Example included performing a HAZOP after preparation of PIDs, the project management team (formed by EC and the direct client Design Institute) has decided to exclude this activity due to schedule and budget constraints. This confirms once more the findings documented below in 3.2.4.2 “Implementing a Safety Policy”.

In the following paragraphs, first examples of lower-level operation requirements and design constraints as well as design features (Level 2 intent specification), also derived in the frame of the trade studies referred in the precious points, are provided. The second part of this point focuses on refining the high-level safety constraint SC.4: *Fire and explosion events must be prevented. [H.4]* by applying STPA and comparing results to the safety-related design features proposed for the Komsomolsk – De-Kastri Project.

Examples of lower-level requirements, design constraints and design features

Table 18 lists examples of lower-level operation requirements and design constraints which have been derived for the design of the Komsomolsk – De-Kastri Project while performing trade studies.

	Some Lower Level Operation Requirements and Design Constraints for Project Example
OP.11	*Contaminate Mix Zone of Diesel Fuel and Naphtha must be divided in 2 parts of equal volume at the middle of the mixing zone. The first part must be routed to a first contaminate tank (Naphtha Diesel Mix) and the second part must be routed to a second contaminate tank (Diesel Naphtha Mix) (→Multiproduct Technology Study [13], ↓2.19)*
OP.12	*The mixture in the Naphtha Diesel Contaminate Tank must be re-injected into the Naphtha stream for export. The mixture in the Diesel Naphtha Contaminate Tank must be re-injected into the Diesel stream. (→Multiproduct Technology Study [13])*

	Some Lower Level Operation Requirements and Design Constraints for Project Example
OP.13	*Contaminate Mix Zone of Diesel Fuel and Jet A1 Fuel must be divided in 2 parts of equal volume at the middle of the mixing zone. The first part must be routed to a first contaminate tank (Jet A1 Diesel Mix) and the second part must be routed to a second contaminate tank (Diesel Jet A1 Mix) (→Multiproduct Technology Study [13], ↓2.19)*
OP.14	*The mixture in the Jet A1 Diesel Contaminate Tank must be re-injected into the Diesel stream. (→Multiproduct Technology Study [13])*
OP.15	*A part of the mixture in the Diesel Jet A1 Contaminate Tank must be re-injected into the Naphtha stream, while the other part must be re-injected into the Diesel stream. The specific quantities shall be specified by the Operator. (→Multiproduct Technology Study [13])*
OP.16	*Main Head Pumps shall pump the largest possible batch of a single oil product. (→Oil Product Transportation Study [12], ↑C.24)*
OP.17	*Main Head Pumps shall pump a batch of the required oil product according to demand forecast. (→Oil Product Transportation Study [12])*
OP.18	*De-Kastri Port shall not follow a Spot-Selling policy, but a Scheduled-Selling policy. (→Oil Product Transportation Study [12]*
OP.19	*A Stand Still time of 6 hours must be allowed for Tanks in De Kastri tank farm only between end of tank filling and beginning of tanker loading (→Oil Product Transportation Study [12])*
OP.20	*A Settling time of 24 hours must be allowed for Jet A1 Tanks in De Kastri tank farm only between end of Stand Still time and beginning of tanker loading (→Oil Product Transportation Study [12])*

Table 18: Examples of Lower-level Operation Constraints derived for the Komsomolsk – De-Kastri Project [12], [13]

Table 19 lists examples of design features which have been derived for the design of the Komsomolsk – De-Kastri Project while performing trade studies.

	Some Design Features for Project Example
2.1	*The pipeline system section I Diesel Fuel line shall provide Outer Diameter (OD) 273 mm and Wall Thickness (WT) 6 mm. (→Pipeline System Selection Study [11], ↑C.6)*
2.2	*The pipeline system section I Naphtha line shall provide Outer Diameter (OD) 245 mm and Wall Thickness (WT) 6 mm. (→Pipeline System Selection Study [11], ↑C.6)*
2.3	*The pipeline system section I Jet A1 Fuel line shall provide Outer Diameter (OD) 178 mm and Wall Thickness (WT) 6 mm. (→Pipeline System Selection Study [11], ↑C.6)*

	Some Design Features for Project Example
2.4	*The pipeline system section II shall provide Outer Diameter (OD) 530 mm and Wall Thickness (WT) 7.72 mm. (→Pipeline System Selection Study [11], ↓L1, L4)*
2.5	*The pipeline system section III Diesel Fuel line shall provide Outer Diameter (OD) 720 mm. (→Pipeline System Selection Study [11], ↑C.6)*
2.6	*The pipeline system section III Naphtha line shall provide Outer Diameter (OD) 720 mm. (→Pipeline System Selection Study [11], ↑C.6)*
2.7	*The pipeline system section III Jet A1 Fuel line shall provide Outer Diameter (OD) 630 mm. (→Pipeline System Selection Study [11], ↑C.6)*
2.8	*Head Tank Farm Total Nominal Volume shall be 280 000 m^3. (→Oil Product Transportation Study [12])*
2.9	*Diesel Fuel Flowrate in pipeline system section I shall be 372 m^3/h. (→Oil Product Transportation Study [12])*
2.10	*Naphtha Flowrate in pipeline system section I shall be 314 m^3/h. (→Oil Product Transportation Study [12])*
2.11	*Jet A1 Fuel Flowrate in pipeline system section I shall be 141 m^3/h. (→Oil Product Transportation Study [12])*
2.12	*Head Tank Farm Diesel Fuel configuration shall be 4 tanks of nominal volume 25,000 m^3/each. (→Oil Product Transportation Study [12])*
2.13	*Head Tank Farm Naphtha configuration shall be 4 tanks of nominal volume 25,000 m^3/each. (→Oil Product Transportation Study [12])*
2.14	*Head Tank Farm Jet A1 Fuel configuration shall be 4 tanks of nominal volume 20,000 m^3/each. (→Oil Product Transportation Study [12])*
2.15	*De-Kastri Tank Farm Total Nominal Volume shall be 320 000 m^3. (→Oil Product Transportation Study [12])*
2.16	*De-Kastri Tank Farm Diesel Fuel configuration shall be 4 tanks of nominal volume 30,000 m^3/each. (→Oil Product Transportation Study [12])*
2.17	*De-Kastri Tank Farm Naphtha configuration shall be 5 tanks of nominal volume 20,000 m^3/each. (→Oil Product Transportation Study [12])*
2.18	*De-Kastri Tank Farm Jet A1 Fuel configuration shall be 5 tanks of nominal volume 20,000 m^3/each. (→Oil Product Transportation Study [12])*
2.19	*De-Kastri Tank Farm shall provide 4 Contaminate Tanks of nominal volume 900 m^3/each. (→Multiproduct Technology Study [13], ↑OP.11, OP.13)* **Assumption:** Mixing zone volumes are expected in the order of magnitude of 300 m^3 each. Each mixing zone is routed into 2 contaminate tanks (150 m^3 each as dedicated mixing zone). Each contaminate tank is assumed to be able to handle 6 dedicated mixing zones. This figure takes into account the scenario in which some unexpected events would prevent re-injection.

	Some Design Features for Project Example
2.20	*De-Kastri Tank Farm shall provide 2 Jet A1 Fuel Buffer Tanks of nominal volume 900 m^3/each. (→Multiproduct Technology Study [13], ↑C.23)* **Assumption:** Buffer batches are assumed in the order of magnitude of 300 m^3 each. Each buffer tank is assumed to be able to handle 3 buffer batches.

Table 19: Examples of Design Features identified for the Komsomolsk – De-Kastri Project [11], [12], [13]

It is interesting to observe that the requirements and constraints listed in Table 16, Table 18 and Table 19 have not found their way into a revision of the Basis of Design of the Komsomolsk – De-Kastri Project [14] (i.e. the reference has not been provided in the captions). This confirms the answers of the review team.

STPA for refining SC.4: "Fire and explosion events must be prevented"

The following analysis is based on typical pipeline system control principles documented:

- Specifically for the "Oil Product Pipeline Komsomolsk – De-Kastri" in the "Operation and Control Philosophy" [18].
- Generally for other pipeline systems such as the "Burgas-Alexandroupolis Crude Oil Pipeline Project" in "Overall Operating and Control Concept" [19] and "Operating and Control Philosophy" [20].

The control principles and information used herein are not complete and might deviate from the latest Project specific decisions taken about operations (e.g. a significant uncertainty during the design process is who will be the operator of the pipeline system. Here it is assumed that a different organization –not the Komsomolsk Refinery– will be the operator). The analysis below is only intended for illustration of what can be done and how the techniques can help.

Brief description of Concept of Operations

The purpose of the Komsomolsk – De Kastri Oil Product Pipeline Project is to transport oil products (i) Diesel Fuel, (ii) Naphtha and (iii) Jet Fuel produced in the Refinery Komsomolsk to other destinations in Far East Russia, as well as to Pacific Rim Markets.

For this purpose the pipeline system foresees the following installations as illustrated in Figure 8:

- Pumping station and metering system in the Komsomolsk Refinery area,
- Dedicated lines, one per product, from Komsomolsk Refinery to THP of approximately 6.4 kilometers,
- Head tank farm and Pump Station,
- Cross-country multiproduct pipeline of approximately 326.6 kilometers,
- De-Kastri Export Terminal including a Tank Farm, loading pumps, a metering system, dedicated loading lines of approximately 3.3 kilometers and a sea island loading point for tanker loading operations.

The system flow diagram provided in Figure 8 can be simplified as illustrated in the block diagram of

Figure 9.

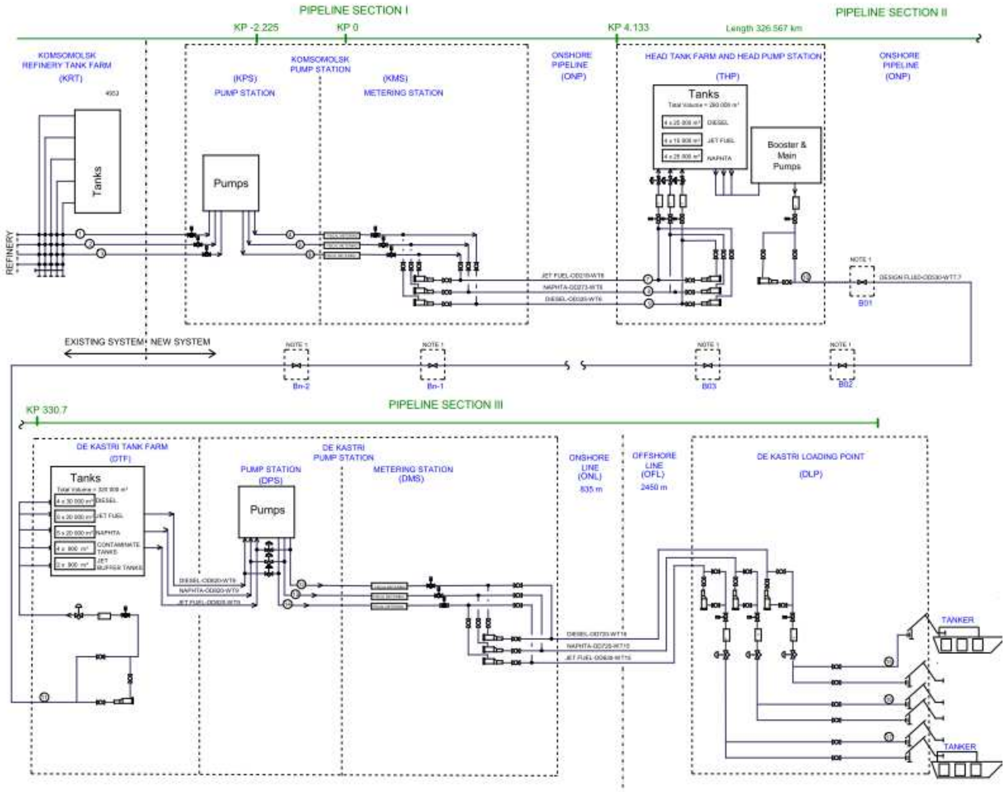


Figure 8: Revised System Flow Diagram of “Oil Product Pipeline Komsomolsk – De-Kastri” [17]

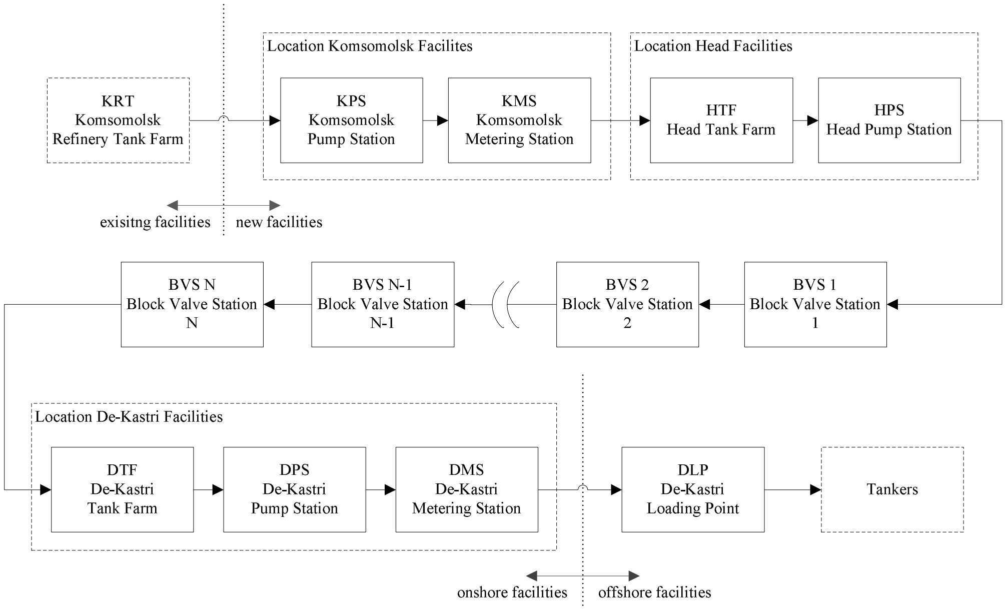


Figure 9: Simplified System Block Diagram for “Oil Product Pipeline Komsomolsk – De-Kastri”

Preliminary System Control Structure

Pipeline system control is basically carried out at two levels:

- At System level (remotely from a Main Control Centre, MCC),
- At Station level, which actually means at location level because Local Control Centers (LCC) are provided in the different locations (e.g. LCC at the Head Facilities controls the processes in the tank farm and in the pump station).

Typical safety-critical systems foreseen for control of fire and explosion hazards in pipeline systems are:

- At System level:
    - Leak Detection System (LDS),
    - Emergency Shut Down System (ESD) push button to initiate Local ESDs. Automatic procedure initiated remotely by operator at MCC. The purpose of the ESD System is to shut down units or stations in safety-critical situations.
    - Controlled Operation ESD (COESD) for the whole system (e.g. in case of confirmed leak detection along the pipeline system). Manual procedure executed remotely by operator at MCC.
- At Station level (Integrated Control and Safety System (ICSS)):
    - Station Control System (SCS)
        - Pressure Control System
        - Leak Detection System (LDS)
    - Emergency Shut Down System (ESD). Automatic procedure initiated either automatically or by operator via push down button.
    - Fire and Gas Detection System (F&G)

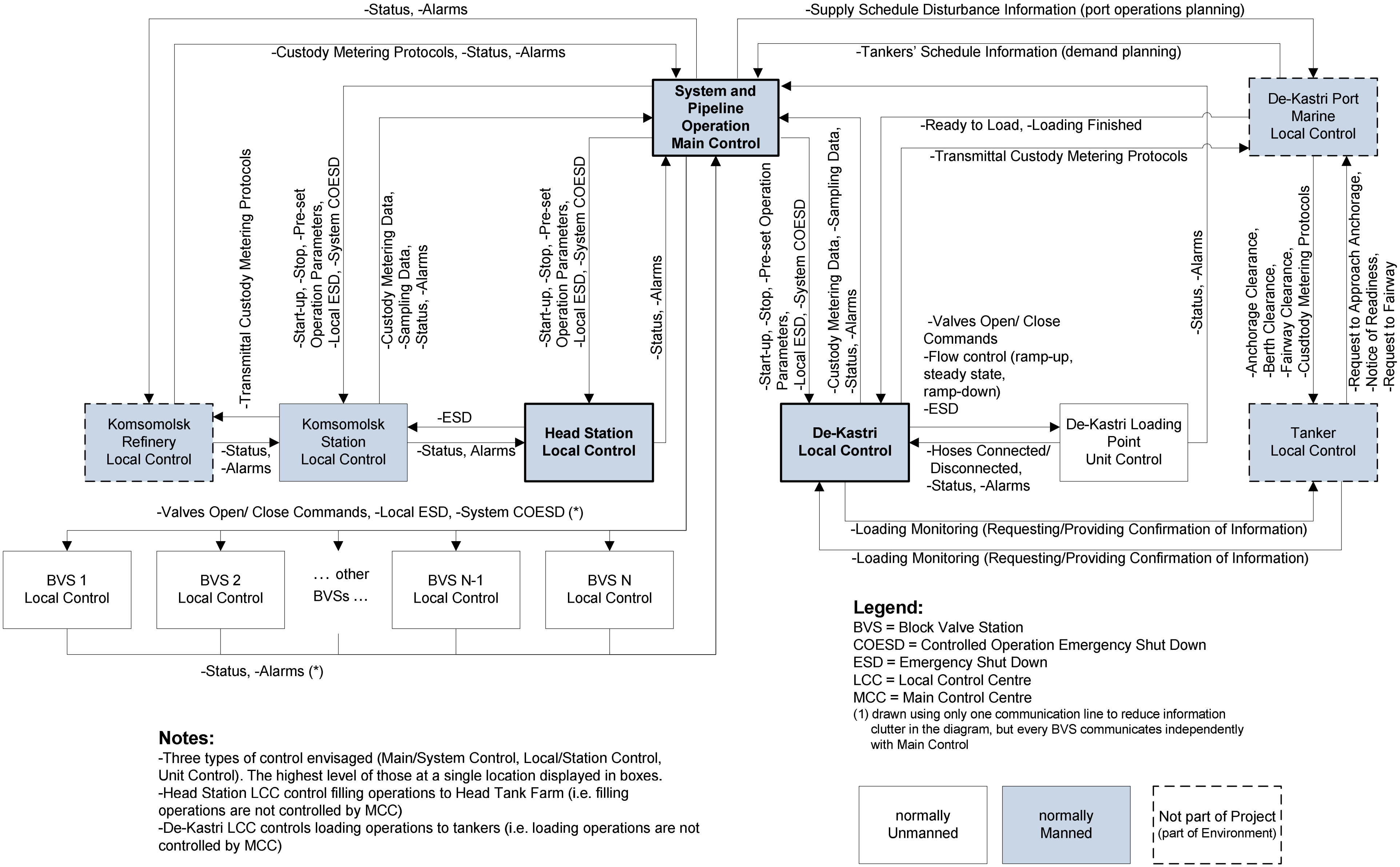
      The purpose of the F&G System is to detect flammable gases, smoke and heat within the shelters and compounds in the pipeline system.
    - Fire Fighting System (only in some stations/ locations)
    - Intrusion Detection System

The fire and explosion hazard control systems listed above are typically classified as:

- Prevention (ESD, Pressure Control System and Flow Path Supervision System),
- Detection (LDS, F&G, Intrusion Detection System),
- Mitigation –protection– (ESD, Fire Fighting System, COESD).

The high-level system control structure is provided in Figure 10.

The normal system operation mode is the “Pipeline Automatic Mode” which is the control mode with the highest level of automation. System and pipeline control is performed from the MCC. Basically the MCC starts the automatic programs which manage the Local Controls at the different locations/ stations:


-Status, -Alarms
-Custody Metering Protocols, -Status, -Alarms
-Supply Schedule Disturbance Information (port operations planning)
-Tankers' Schedule Information (demand planning)
System and Pipeline Operation Main Control
De-Kastri Port Marine Local Control
-Ready to Load, -Loading Finished
-Transmittal Custody Metering Protocols
-Transmittal Custody Metering Protocols
-Start-up, -Stop, -Pre-set Operation Parameters, -Local ESD, -System COESD
-Custody Metering Data, -Sampling Data, -Status, -Alarms
-Start-up, -Stop, -Pre-set Operation Parameters, -Local ESD, -System COESD
-Status, -Alarms
-Start-up, -Stop, -Pre-set Operation Parameters, -Local ESD, -System COESD
-Custody Metering Data, -Sampling Data, -Status, -Alarms
-Valves Open/ Close Commands
-Flow control (ramp-up, steady state, ramp-down)
-ESD
-Status, -Alarms
-Anchorage Clearance, -Berth Clearance, -Fairway Clearance, -Custdtody Metering Protocols
-Request to Approach Anchorage, -Notice of Readiness, -Request to Fairway
Komsomolsk Refinery Local Control
-Status, -Alarms
Komsomolsk Station Local Control
-ESD
-Status, Alarms
Head Station Local Control
De-Kastri Local Control
-Hoses Connected/ Disconnected, -Status, -Alarms
De-Kastri Loading Point Unit Control
Tanker Local Control
-Valves Open/ Close Commands, -Local ESD, -System COESD (*)
-Loading Monitoring (Requesting/Providing Confirmation of Information)
-Loading Monitoring (Requesting/Providing Confirmation of Information)
BVS 1 Local Control
BVS 2 Local Control
… other BVSs …
BVS N-1 Local Control
BVS N Local Control
-Status, -Alarms (*)
normally Unmanned
normally Manned
Not part of Project (part of Environment)

Legend:

BVS = Block Valve Station
COESD = Controlled Operation Emergency Shut Down
ESD = Emergency Shut Down
LCC = Local Control Centre
MCC = Main Control Centre
(1) drawn using only one communication line to reduce information clutter in the diagram, but every BVS communicates independently with Main Control

Notes:

-Three types of control envisaged (Main/System Control, Local/Station Control, Unit Control). The highest level of those at a single location displayed in boxes.
-Head Station LCC control filling operations to Head Tank Farm (i.e. filling operations are not controlled by MCC)
-De-Kastri LCC controls loading operations to tankers (i.e. loading operations are not controlled by MCC)

Figure 10: High-Level System Control Structure of "Oil Product Pipeline Komsomolsk – De-Kastri".

- The MCC interfaces with the external control units (i.e. controllers not part of the new transportation system), which are (i) the “Refinery Komsomolsk LCC” upstream and (ii) the “De-Kastri Port Marine Control Centre” downstream.
    - The Refinery LCC and the MCC exchange information about status and alarms in their facilities, but none can initiate ESD actions on the facilities of the other. The Refinery Komsomolsk owns the products transported and the booster pump station, metering and sampling station located in the “Komsomolsk Station”, see Figure 10. That is why the Custody Metering Protocols are issued by the Refinery Komsomolsk to the MCC (i.e. to the pipeline operator).
    - Planning information as well as notification of production disturbances are exchanged between the MCC and the Port Control. This is a control on a very high level and on a monthly/ weekly basis (i.e. high-level transportation system scheduling).
- The MCC provides commands to the Local Controls for:
    - Start-up and stop operations (e.g. flow increase/ decrease),
    - Pre-set of process parameters (e.g. pump stations flowrate or suction pressure at pump stations),
    - Remote control of equipment changeover at the locations (e.g. between essential equipment groups such as pump trains or metering trains),
    - Initiation of Local automatic ESD actions in the different locations as well as manually Controlled Operation ESD (COESD) for the whole system (e.g. in case of confirmed leak detection along the pipeline system).

  And receives information from the Local Controls on status of equipment and process parameters, as well as alarms.
- The MCC remotely controls the pipeline and its Block Valve Stations (BVS), receiving back information on status of equipment and process parameters, as well as alarms.

Station/ Local Control is performed from the different LCCs. These interface mainly with the MCC, but some can also interface with other Local Controls as for the case of the “Head LCC” and the “De-Kastri LCC”. For example, the “De-Kastri LCC” performs the control of the loading operations. These two LCCs also perform very important controls at the station level like the tank farms control and the product quality control. These are not illustrated in Figure 10.

Between the safety-critical systems listed above, the ESD System has been selected for further analysis because it is one of the systems on which project teams over-rely and focus the most during the SIL Assessments (i.e. “the ESD System will prevent all kinds of hazards when others have failed to do so”).

There are typically four ESD-levels:

- ESD-Level 1: Overall System Shutdown. This is normally not envisaged for this type of systems.
- ESD-Level 2: Multiple Station Shutdown. Initiation of Local automatic ESD actions, possible from MCC only.

  - Loading Operation Shutdown
  - Main Pipeline Shutdown
  - Filling Operation Shutdown
- ESD-Level 3: Single Station Shutdown. Initiation of Local automatic ESD actions, possible (i) automatically by ESD System, (ii) remotely from MCC, (iii) locally from LCC and (iv) manually in the field –ESD push buttons–.

  ESD-Level 3 actions at Head Station and De-Kastri Station include: (i) Trip Pump, (ii) Close Station Inlet/ Outlet ESD Valves, (iii) Isolate Tanks and (iv) Trip Upstream Pumps.
  - Komsomolsk Station
  - Head Station
  - BVSs
  - De-Kastri Station
- ESD-Level 4: Part/section of a Station Shutdown. Initiation of Local automatic ESD actions, possible (i) automatically by ESD System, (ii) remotely from MCC, (iii) locally from LCC and (iv) manually in the field –ESD push buttons–.

  ESD-Level 4 actions trigger only Pump Trip.

The system control structure presented in Figure 11 illustrates the control in one general station/ location and the interface with the MCC and the controlled process. Examples of loops triggering ESD-Level 3 and ESD-Level 4 have been illustrated. For simplification purposes no control actions have been displayed to/ from interfacing stations/ LCCs, although the "Head LCC" and the "De-Kastri LCC" execute some, as explained above. In "Pipeline Automatic Mode" steady-state operation, intervention from the operators is not envisaged, except by using the shutdown push buttons in case of emergency, which triggers the Local ESDs. The control structure of Figure 11 displays the safety-critical systems listed above and their interfaces to the ESD system. Only some examples of signals triggering ESD-Level 3 and Level 4 actions have been provided. The details of Figure 11 are self-explanatory.

Hazard Analysis and Generation of Safety Requirements and Constraints

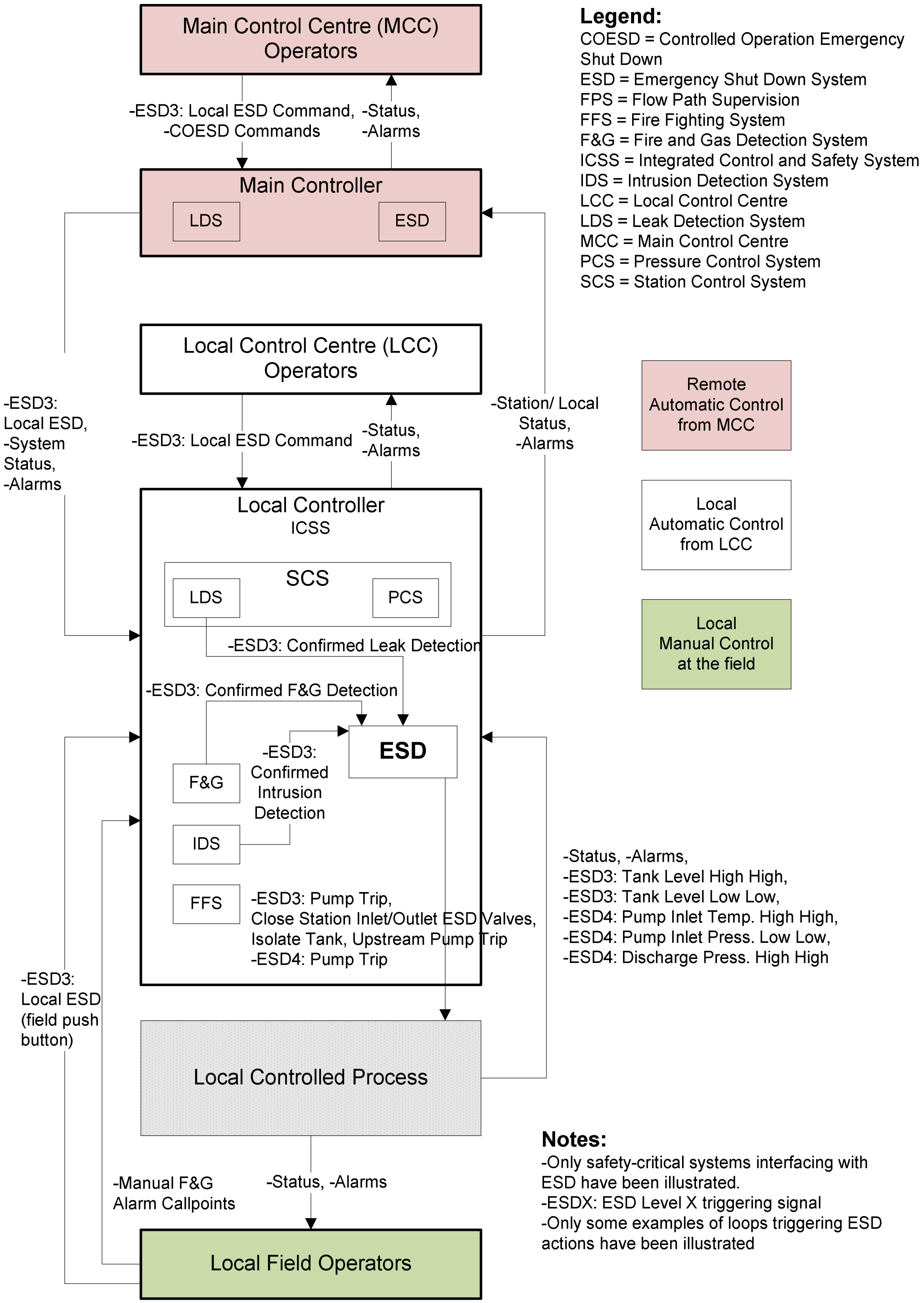
The high-level hazard of concern in this analysis is:

H.4: "*Fire and/ or explosion events*"

1. Identifying Unsafe Control Actions (UCAs)

The first step of STPA, once a control structure is characterized, is to identify possible Unsafe Control Actions the controllers might execute. According to Figure 11, there are five controllers who can trigger and/ or execute ESD actions:

- Operators in MCC (Human Controllers)
- Main Controller (Automated Controller)
- Operators in LCC (Human Controllers)
- Local Controller (Automated Controller)
- Operators in the field (Human Controllers)



Legend:

COESD = Controlled Operation Emergency Shut Down
ESD = Emergency Shut Down System
FPS = Flow Path Supervision
FFS = Fire Fighting System
F&G = Fire and Gas Detection System
ICSS = Integrated Control and Safety System
IDS = Intrusion Detection System
LCC = Local Control Centre
LDS = Leak Detection System
MCC = Main Control Centre
PCS = Pressure Control System
SCS = Station Control System

Notes:

-Only safety-critical systems interfacing with ESD have been illustrated.
-ESDX: ESD Level X triggering signal
-Only some examples of loops triggering ESD actions have been illustrated

Figure 11: Pipeline System ESD Control Structure for a General Station of "Oil Product Pipeline Komsomolsk – De-Kastri"

The following analysis will focus on the Local Controller, which as displayed in Figure 11, is responsible for a good part of the processing of safety-critical signals and execution of actions. Table 21 identifies Unsafe Control Actions by the Local Controller. This table has been generated following the methodology explained in Chapters 4 and 8 of Leveson's "Engineering a Safer World" [1] which is based on the fact that control actions can be hazardous in four ways:

- A control action required for safety is not provided or not followed.
- An Unsafe Control Action is provided that leads to a hazard.
- A potentially safe control action is provided too late, too early, or out of sequence.
- A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action).

Eleven (11) Unsafe Control Actions have been identified.

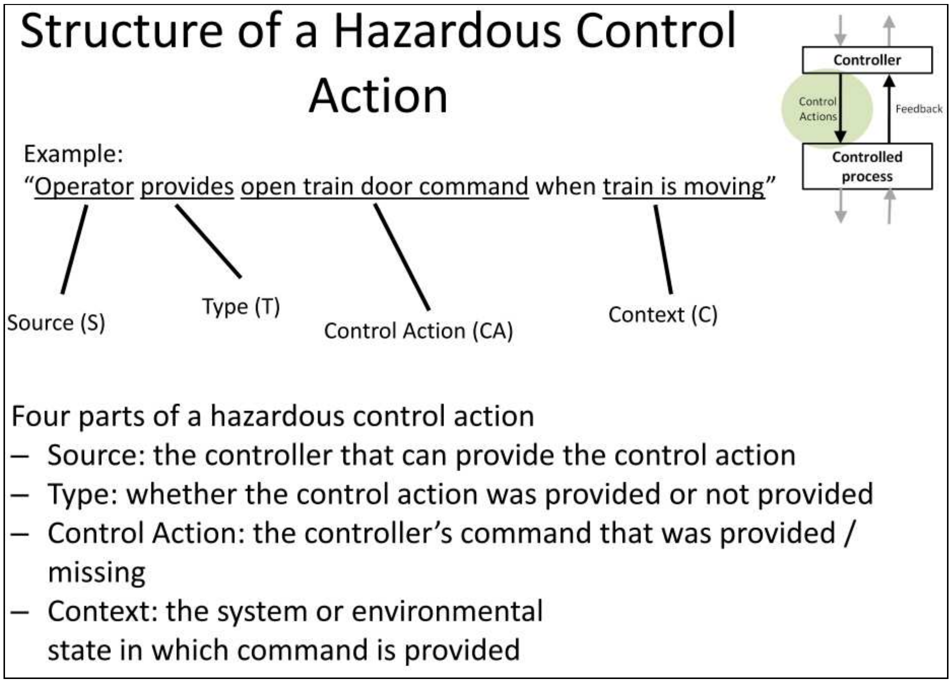
	Unsafe Control Actions of Local Controller on ESD Procedures
UCA-LC.1	ESD3 actions not provided when required.
UCA-LC.2	ESD3 actions provided, but executing in the wrong components.
UCA-LC.3	ESD3 actions provided too late.
UCA-LC.4	ESD3 actions provided out of sequence.
UCA-LC.5	ESD3 actions provided, but stopped too early.
UCA-LC.6	ESD4 actions not provided.
UCA-LC.7	ESD4 actions provided too late.
UCA-LC.8	ESD4 actions provided out of sequence.
UCA-LC.9	ESD4 actions provided, but stopped too early.
UCA-LC.10	Confirmed leak detection or confirmed fire or gas detection or confirmed intrusion detection not provided. **Remark:** This should be broken into 3 SCs in real life.
UCA-LC.11	Confirmed leak detection or confirmed fire or gas detection or confirmed intrusion detection provided too late. **Remark:** This should be broken into 3 SCs in real life.

Table 20: List of identified Unsafe Control Actions of Local Controller on ESD procedures in a General Station of "Oil Product Pipeline Komsomolsk – De-Kastri"

These Unsafe Control Actions should be translated into safety constraints on the Local Controller. In order to generate more precise safety constraints (e.g. not only specifying "ESD3 actions must be provided when required"), the "Structure of Hazardous Control Actions" proposed by Thomas would help. See Figure 12 below.

Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Wrong Timing/ Order Causes Hazard**	**Stopped Too Soon or Applied Too Long Causes Hazard**
STPA-LC.1 **ESD3: Pump Trip, Close Station Inlet/ Outlet Valves, Isolate Tanks, Upstream Pump Trip**	Not providing would lead to a major accident because the quantities of hydrocarbon released would be very high and active and passive protecting systems would not cope with the fires generated evolving into a major explosion – unsafe	-Providing when not required basically would only lead to loss of operation – not unsafe -Providing confusing valves to close, for example, could lead to overpressures potentially causing LOC – unsafe	-Providing too early would only lead to loss of operation – not unsafe -Providing too late might allow enough time for formation of flammable mixture and ignition – unsafe -Providing out of sequence (e.g. close station inlet/ outlet before tripping pump) would lead to overpressures potentially causing LOC – unsafe	-Interrupting pump trips or leaving valves partially open would allow for formation of flammable mixture and ignition – unsafe -Providing too long not relevant – not unsafe
STPA-LC.2 **ESD4: Pump Trip**	Not providing might cause cavitation in the pumps and eventually overpressures potentially causing LOC – unsafe	Providing when not required basically would only lead to loss of operation – not unsafe	-Providing too early would only lead to loss of operation – not unsafe -Providing too late might cause cavitation in the pumps and eventually overpressures potentially causing LOC – unsafe -Providing out of sequence (i.e. wrong order in pump trip steps) might lead to cavitation in the pumps and eventually overpressures potentially causing LOC – unsafe	Interrupting pump trips might lead to cavitation in the pumps and eventually overpressures potentially causing LOC – unsafe -Providing too long not relevant – not unsafe
STPA-LC.3 **Confirmed Leak or F&G or Intrusion Detection to initiate ESD3**	Not providing would cause formation of flammable mixture and ignition – unsafe **Assumption:** intruders' objective is to perform hot-tap and steal products for re-selling.	Providing when not required basically would only lead to loss of operation – not unsafe	-Providing too early would only lead to loss of operation – not unsafe -Providing too late might allow enough time for formation of flammable mixture and ignition – unsafe -Providing out of sequence not relevant (discrete events) – not unsafe	Not relevant (discrete events) – not unsafe

Table 21: Unsafe Control Actions of Local Controller on ESD procedures in a General Station of "Oil Product Pipeline Komsomolsk – De-Kastri"



Structure of a Hazardous Control Action

Example:
"Operator provides open train door command when train is moving"

Four parts of a hazardous control action

- Source: the controller that can provide the control action
- Type: whether the control action was provided or not provided
- Control Action: the controller's command that was provided / missing
- Context: the system or environmental state in which command is provided

Figure 12: Structure of a Hazardous Control Action [22]

This way for example UCA-LC.1 "ESD3 actions not provided when required" would be translated into the following UCAs which have been derived by observing Figure 11:

	Unsafe Control Actions derived from UCA-LC.1
UCA-LC.1-1	Local Controller does not provide ESD3 Control Actions when Tank Level has reached High High.
UCA-LC.1-2	Local Controller does not provide ESD3 Control Actions when Tank Level has reached Low Low.
UCA-LC.1-3	Local Controller does not provide ESD3 Control Actions when Confirmed Leak Detection.
UCA-LC.1-4	Local Controller does not provide ESD3 Control Actions when Confirmed Fire or Gas Detection.
UCA-LC.1-5	Local Controller does not provide ESD3 Control Actions when Confirmed Intrusion Detection.
UCA-LC.1-6	Local Controller does not provide ESD3 Control Actions when Local Operator has pushed ESD push button in the field.
UCA-LC.1-7	Local Controller does not provide ESD3 Control Actions when Local Operator has pushed ESD push button in the LCC.
UCA-LC.1-8	Local Controller does not provide ESD3 Control Actions when Main Controller has provided Local ESD Command.

Table 22: List of Unsafe Control Actions derived from UCA-LC.1 "ESD3 actions not provided when required" in a General Station of "Oil Product Pipeline Komsomolsk – De-Kastri"

Then the safety-constraints generated would be much more precise and complete:

	Safety-Constraints generated from UCA-LC.1
SC-LC.1	Local Controller must provide ESD3 Control Actions when Tank Level has reached High High. (→STPA-LC.1)
SC-LC.2	Local Controller must provide ESD3 Control Actions when Tank Level has reached Low Low. (→STPA-LC.1)
SC-LC.3	Local Controller must provide ESD3 Control Actions when Confirmed Leak Detection. (→STPA-LC.1)
SC-LC.4	Local Controller must provide ESD3 Control Actions when Confirmed Fire or Gas Detection. (→STPA-LC.1)
SC-LC.5	Local Controller must provide ESD3 Control Actions when Confirmed Intrusion Detection. (→STPA-LC.1)
SC-LC.6	Local Controller must provide ESD3 Control Actions when Local Operator has pushed ESD push button in the field. (→STPA-LC.1)
SC-LC.7	Local Controller must provide ESD3 Control Actions when Local Operator has pushed ESD push button in the LCC. (→STPA-LC.1)
SC-LC.8	Local Controller must provide ESD3 Control Actions when Main Controller has provided Local ESD Command. (→STPA-LC.1)

Table 23: Derived Safety Constraints on Local Controller for prevention of UCA-LC.1 “ESD3 actions not provided when required” in a General Station of “Oil Product Pipeline Komsomolsk – De-Kastri”

The same should be performed with the other Unsafe Control Actions identified, so that a comprehensive set of precise safety constraints would be generated.

2. *Determining Causes of Identified Unsafe Control Actions*

The second step of STPA, once the Unsafe Control Actions have been identified, is to find their potential causes so that ultimately lower-level safety constraints can be defined to prevent them. Table 24 has been generated following the methodology explained in Chapters 4 and 8 of Leveson’s “Engineering a Safer World” [1] and the case study explained in “Safety Assurance in NextGen” [21]. Only causes of the first Unsafe Control Action identified UCA-LC.1 “ESD3 actions not provided when required” have been analyzed for illustration purposes. Ideally, the refined UCAs of Table 23 should be analyzed though.

Figure 13 provides a general control loop and the simplified types of causes (control flaws) to be investigated which might cause Unsafe Control Actions. In this case, as in [21], the arrow between controller and actuator does not include further detail as inappropriate, ineffective and missing control action has been addressed in STPA Step 1 above. Likewise, the arrow between actuator and controlled process on delayed operation is not relevant for UCA-LC.1 “ESD3 actions not provided when required”.

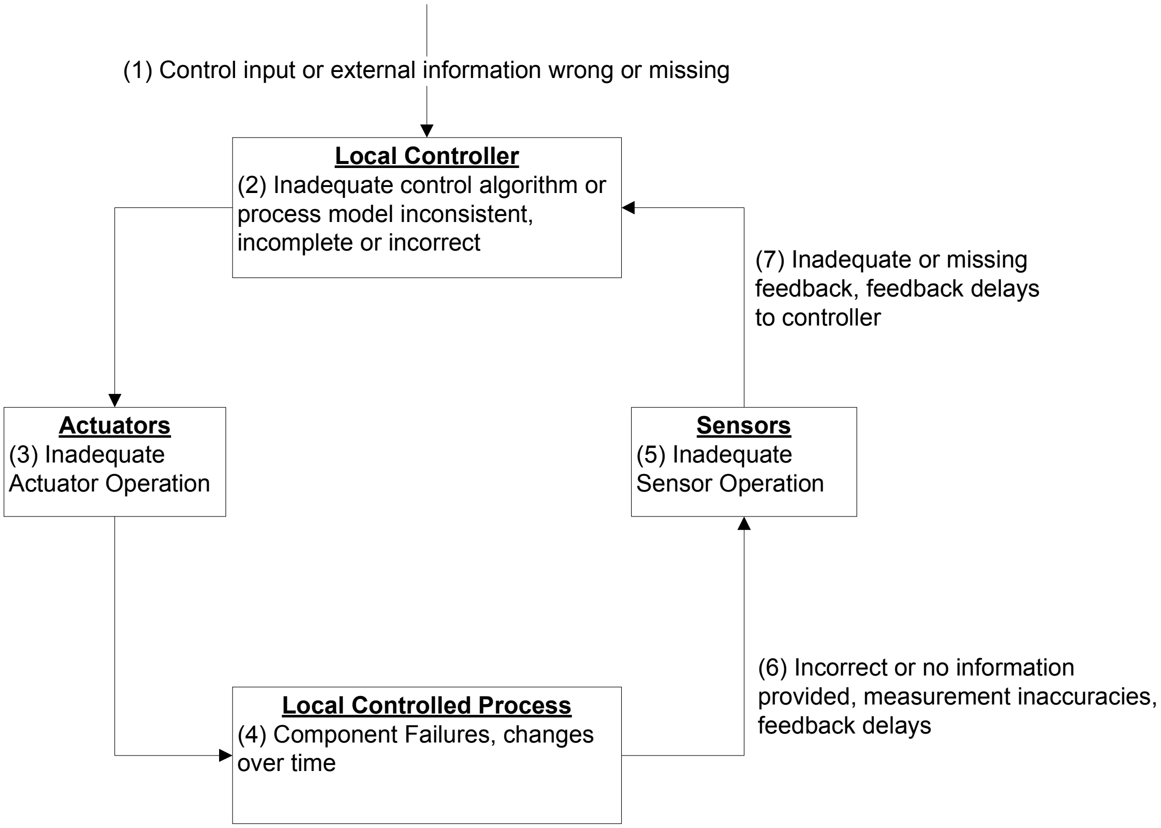

(1) Control input or external information wrong or missing
Local Controller
(2) Inadequate control algorithm or process model inconsistent, incomplete or incorrect
(7) Inadequate or missing feedback, feedback delays to controller
Actuators
(3) Inadequate Actuator Operation
Sensors
(5) Inadequate Sensor Operation
(6) Incorrect or no information provided, measurement inaccuracies, feedback delays
Local Controlled Process
(4) Component Failures, changes over time

Figure 13: General Control Loop for Local Controller with Simplified Types of Causes of Unsafe Control Actions, adapted from [1] and [21]

Table 24 identifies examples of possible causes for UCA-LC.1 "ESD3 actions not provided when required" based on the information of Figure 11.

Hazard H.4 "Fire and/or Explosion" **Unsafe Control Action "ESD3 actions not provided when required"**	
Process Model Link	**Causes**
(1) Control Input or External Info. Wrong or Missing	-Confirmed Leak Detection not provided by LDS. **Remark:** ESD is usually independent from SCS to avoid common cause failures. The so-called ICSS includes the SCS and the so-called Fail Safe Systems (ESD, F&G, IDS, FFS). LDS is usually part of SCS. -Confirmed F&G Detection not provided by F&G. -Confirmed Intrusion Detection not provided by IDS. -Local ESD command not provided by Local Operator at LCC or field. -Local ESD command not provided by Main Controller.

Hazard H.4 “Fire and/or Explosion”
Unsafe Control Action “ESD3 actions not provided when required”

Process Model Link	**Causes**
(2) Inadequate Control Algorithm. Process Model Inconsistent, incomplete or wrong	*Causes of Inadequate Control Algorithm:* -Requirements not passed to designers/ developers or incompletely specified. -Manufacturer’s re-use of standard control algorithms without complete check of adequacy for project specifics. -Control algorithms do not account for feedback loop delays. -Requirements not implemented correctly in software. -Controller components deterioration over time. *Examples of Process Model Incompleteness/ Inconsistencies:* -Simultaneous requests/ commands for Local ESD (e.g. initiated by Local Operator in LCC and by Local Operator in the field) may be provided and the Process Model may not include this scenario. -Controller understanding of tank level signals is wrong. -Controller understanding of Confirmed Detections (LDS, F&G, IDS) is wrong.
(3) Inadequate Actuator Operation	-Communication channel to valves’ actuators becomes corrupted. -Power failure. -Valves’ actuators failures/ degradation over time.
(4) Component Failures/ Changes Over Time	-Valves’ failures/ degradation over time. Pumps failures/ degradation over time (e.g. cavitation). -Failures/ degradation over time of valves’ position monitoring components. -Components’ replacement or environment changes by maintenance operations. -Power failure.
(5) Inadequate Sensor Operation	-Datalink becomes corrupted. -Failures/ degradation over time of tanks’ level transmitters. -Power failure.
(6) Incorrect or No Information Provided, Measurement Inadequacies, Feedback Delays	-Failures/ degradation over time of tanks’ level gauges.

Hazard H.4 “Fire and/or Explosion” **Unsafe Control Action “ESD3 actions not provided when required”**	
Process Model Link	**Causes**
(7) Inadequate or Missing Feedback to Controller, Feedback Delays	-Feedback on tanks’ level not provided. Wrong tanks’ level is transmitted. -Power failure.

Table 24: Analysis of Possible Causes leading to “ESD3 actions not provided when required”

These causes can be translated again in lower-level safety constraints to be considered when designing the Local Controller and its components. Some causes of UCAs can be investigated in more detail so that requirements can be generated more precisely and specifically for the project, or the requirement for investigation may be “transferred” (i.e. risk transfer strategy) to component manufacturers.

Discussion

The requirements for the ESD System (which is an element of the Local Controller) captured in the “Operation and Control Philosophy” [18] prepared for the “Oil Product Pipeline Komsomolsk – De-Kastri” are listed as follows:

	System-Level Requirements for the ESD System
LC-ESD.1	*The ESD System shall provide redundancy for all components whose failure would result in loss of control, data or operator interfaces.*
LC-ESD.2	*The Station ESD System shall be connected to Pump Units ESD System to ensure shut down of the pump units in the events of process conditions deviations, process trips or operator initiated ESD (push button).*
LC-ESD.3	*The ESD Systems shall be certified according to IEC 61508 SIL 2 (as a minimum).* **Remark:** SIL Assessment has not been performed in the Project.
LC-ESD.4	*The ESD Systems shall be able to operate in a fail-safe configuration.*
LC-ESD.5	*The ESD Systems shall be designed considering typical failure modes. Common cause failure modes shall be eliminated, where practicable.*

Table 25: ESD System requirements specified in “Operation and Control Philosophy” [18] prepared for the “Oil Product Pipeline Komsomolsk – De-Kastri”.

The set of requirements specified in the “Operation and Control Philosophy” [18] is not the result of a hazard analysis. Originally it was planned to perform HAZOP, but as reported above, the project management team (formed by EC and the direct client Design Institute) has decided to exclude this activity due to schedule and budget constraints. Therefore these requirements have been generated following only common industry practice.

The small set of requirements specified in the “Operation and Control Philosophy” [18] seems to put a large emphasis on reliability assurance, while the set of requirements generated using STPA focuses on the identified hazards and their causes. The set of requirements that can be generated with STPA is a lot more comprehensive and precise. While there is no doubt that the quality of the set of requirements obtained with STPA is far better than what it is normally documented in typical Operation and Control Philosophies such as [18], [19] or [20] and the typical specifications of safety-critical systems generated, the desire to generate specifications in such a level of detail so early in the project lifecycle might be arguable, for it seems design organizations do not like to assume too much responsibility during Basic Design and FEED regarding the design to be performed by manufacturers later (regardless of safety-critical or not safety-critical design). On the other hand, the more comprehensive and precise the requirements are, the more accurate prices can be estimated by bidders/ manufacturers and the better the basis on which a contract management/ follow-up can be performed later, therefore overall benefiting the project. This seems to be something to be solved again with a clearly defined Safety Policy.

HAZOP, HAZID and STPA ultimately have in common that they search for causes of deviations of intended behavior to try to manage those (prevent, detect, mitigate). HAZID identifies causes of identified hazardous scenarios, HAZOP identifies causes of process parameters deviations, and STPA identifies causes of hazardous control actions. The type of reasoning involved to arrive to conclusions is rather different from technique to technique (especially because STPA prescribes a systems-theoretic view of causality).

Regarding SIL Assessment, both the objective (i.e. formulate recommendations to achieve a defined target SIL) and the type of reasoning used (i.e. frame provided by IEC 61511) is completely different from STPA. SIL Assessment seems to be rather a risk transfer strategy to the manufacturers at lower levels (i.e. *"The ESD Systems shall be certified according to IEC 61508 SIL 2 as a minimum"),* as opposed to STPA where the reasons why unsafe control actions are executed, are sought. SIL Assessment also seems to be an attempt to create a clear boundary between the responsibility of the systems and sub-systems or components. Instead of trying to find reasons why systems might reach hazardous states in a joint effort, the responsibility and the risk involved is transferred to the manufacturers at lower levels. SIL Assessment does not perform any analysis of causes. It is observed that SIL should be rather interpreted as a quality standard to be delivered by manufacturers (i.e. it is rather about fulfilling a reliability target), not as a safety standard.

Besides the findings discussed above, a practical advantage of STPA is that it can be performed independently by an analyst or by a team of analysts. It does not need a formal panel of experts (as for HAZID or HAZOP), which normally requires extra resources for an organization. Issues such as rank in the organization and dominant personalities typically bias the documentation of results of the exercise (even if the exercise has been contracted to a third party).

While it seems that performing STPA to a satisfactory level of completion can be very lengthy, HAZID, HAZOP and SIL Assessment are not short exercises to perform and it is also difficult to achieve a satisfactory level of completion.

3.2.2.8.4Definition of High-Level Guidelines for Implementation of Step in EC

Safety-related philosophies and safety-related project activities (i.e. hazard analysis such as HAZID, HAZOP, SIL, QRA and meetings for definition or review of safety-related design philosophies) should also be defined as part of contract negotiations.

When trying to expand the scope of HAZID and HAZOP for introduction of elements of STPA (e.g. introducing guidewords/ deviations on enforcement of safety constraints) the chairman should try not to increase the length of the workshops, since this seems to be an issue with managers and project teams.

The recommendations and actions (safety constraints) generated during the hazard analyses performed should be incorporated in the Basis of Design, which should be structured as an intent specification, as repeatedly proposed in other points of this thesis.

Standard operation and control philosophies (like the one used for illustration purposes in the Project Example) as well as specifications of safety-critical systems should be further developed (improved) with the aid of STPA. A policy under consideration of the pros and cons described in the discussion above needs to be developed as to define the level of detail that operation and control philosophies and specifications of safety-critical systems should contain. This decision should be part of the Safety Policy to be developed, see 3.2.4.2 “Implementing a Safety Policy”. In any case, at least having a standard comprehensive set of precise safety-related requirements for systems to be procured would be useful for performing hazard analyses together with manufacturers during Detail Design.

3.2.2.9 Documenting System Limitations

The findings and recommendations documented in 3.2.2.5 “Documenting Environmental Assumptions” can be considered applicable to this section, as identification and documentation of both Environmental Assumptions and System Limitations suffer the same treatment. Both are often considered obvious and not worth being documented by the engineers writing Basis of Design and specifications, but also by the engineering managers and even clients. Both tend to go forgotten between different project phases and teams.

3.2.2.9.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 67 to 71. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting “Documenting system limitations” in column “Element of Using STAMP”.

The review team reported that limitations of systems specified are generally known in the industry. That’s why they are not systematically documented through the development process. For example it is known that leak detection systems cannot detect small leaks. Some interviewees reported that process limits are documented in Basis of Design. Limitations of systems/ components procured are usually documented in specifications. It was noted that performance standards is a good frame to document systems/ components limitations. Design limitations are poorly documented in the hazard analyses performed.

The review team agreed that the importance of design limitations is fundamental for ensuring safe operation.

3.2.2.9.2Feasibility of Step Implementation in EC and By-Products

Leveson identifies four types of typical limitations: (i) related to basic functional requirements, (ii) related to Environmental Assumptions, (iii) related to hazards or hazard causal factors which have not been eliminated or controlled through design and (iv) related to trade-offs made during design. See examples in Table 26.

Since documentation of System Limitations already takes place to some extent (mainly regarding basic functional requirements –Level 1 of intent specification, see Figure 7 and at the system/ component specification level –Level 3 and Level 4, see Figure 7), it seems to be a matter of managing a list of System Limitations (in a similar way as for Environmental Assumptions) as part of an improved Basis of Design understood as an intent specification.

It is considered necessary and feasible to implement this step. Again implementation of this step is expected to not only improve the safety of the engineered systems, but also the efficiency of engineering management activities and the quality of the engineering work delivered.

3.2.2.9.3Development of Step for the Project Example

In a similar way as for Environmental Assumptions, the list of input data part of the Basis of Design [14] included some limitations. Also the studies performed during concept selection (i) Pipeline System Selection Study [11], (ii) Oil Product Logistic Transportation Model Study [12] and (iii) Multiproduct Technology Study aiming to ensure Product Quality [13] (see 3.2.2.4 “Integrating Safety into Architecture Selection and System Trade Studies”) delivered some design limitations. The table below shows some examples.

	Some Limitations for Project Example	**Type**
L1.	*Pipeline Maximum Allowable Operating Pressure is 91.88 barg. (→Pipeline System Selection Study [11], ↑2.4)*	*Trade-off*
L2.	*Minimum Acceptable Operating Pressure is 2 barg. (→Pipeline System Selection Study [11])*	*Functional*
L3.	*Pipeline Minimum Batch Size for oil products is 20,000 m^3. (→Oil Product Transportation Study [12], ↑C.24)*	*Trade-off*
L4.	*Pipeline Maximum Allowable Boost Rate is 2%. (→Oil Product Transportation Study [12], ↑2.4)*	*Trade-off*
L5.	*Maximum Allowable Wind Speed for Tanker Loading Operations is 10 m/s.*	*Uncontrolled Hazard*
L6.	*Maximum Allowable Wave Height for Tanker Loading Operations is 2 m.*	*Uncontrolled Hazard*
L7.	*Multiple berths at the loading point in Port De-Kastri cannot load the same oil product at a time. (→Oil Product Transportation Study [12])*	*Functional*
L8.	*A single tanker at the loading point in Port De-Kastri cannot load multiple oil products at a time. (→Oil Product Transportation Study [12])*	*Functional*

	Some Limitations for Project Example	Type
L9.	*Berth 1 Minimum Capacity is 0 DWT and Maximum Capacity is 40,000 DWT. (→Oil Product Transportation Study [12])*	*Functional*
L10.	*Berth 2 Minimum Capacity is 40,000 DWT and Maximum Capacity is 100,000 DWT. (→Oil Product Transportation Study [12])*	*Functional*

Table 26: Examples of Limitations identified for the Komsomolsk – De-Kastri Project [11], [12], [14]

3.2.2.9.4Definition of High-Level Guidelines for Implementation of Step in EC

Overall the intent should be to handover a valid list of System Limitations to operations at the end of the project Execution phase. EC should promote this practice through the different project phases where it is involved, not only if involved in Execution, but also starting from the Conceptual Design phase.

Limitations related to basic functional requirements and to Environmental Assumptions should be listed right away in the first Basis of Design produced. Then as design progresses limitations related to hazards not controlled and to trade-offs should be gradually added. The review proposed to identify and document System Limitations at defined hold points in the design process (e.g. Gate Reviews), which adequately fits to the idea of treating the Basis of Design as an intent specification.

Documenting System Limitations during hazard analysis could also be implemented right away, at least for the hazard analyses where EC has a chairman role.

3.2.3 Operations

3.2.3.1 Considering Relevant Operations Experience in the Development

3.2.3.1.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 72 to 78. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting “Considering relevant operations experience in the development” in column “Element of Using STAMP”.

In general, an important gap between project groups and operations groups is reported. This gap exists within organizations (i.e. “internal gap” in clients and/ or operators’ organizations) and between organizations (i.e. “external gap” between engineering organizations and operators’ organizations). EC tries to develop knowledge about operations basically by (i) employing personnel with previous experience in operations and (ii) exposing employees to construction and commissioning activities when EC has a supervisory role in the project. Dissemination of this knowledge either does not happen or it is difficult. Documentation on the lessons learned by experienced employees is not easily available, if available at all.

Operations experience is considered in the development process mainly by

- Involving experts with previous experience in operations.
- Using clients’/ operators’ design standards which are developed based on their previous experience operating systems.

- Using the information in the body of knowledge of the Oil & Gas industry.
- Involving the operations units, if exist and if available.
- Organizing lessons learned sessions at the start of projects.
- Sometimes, when performing work for a revamp or an expansion of an existing system, by involving specific individuals of the clients'/ operators' organization which operate the system and which have also been involved when the greenfield project was executed before.

Operations and maintenance engineers are sometimes involved in safety-related activities, typically if they are performed in the form of a workshop (e.g. HAZID, HAZOP or SIL), otherwise not. Field operators are rarely involved in safety-related activities. Normally operations and maintenance units join the projects for commissioning, not before.

Interviewees do not believe that no accidents or losses over a period of time is a valid legitimation of a system design as safe. The review team argues that the hazards inadequately controlled by a certain design might still be compensated (controlled) by very experienced operators (e.g. operator intentionally deviates from defined procedure to control a previously unidentified hazard) or even go unnoticed (e.g. undetected releases dilute or do not find ignition source). Interviewees generally believe accidents can be prevented but some argue it is very difficult to do so.

Past clients and/ or operators only provide feedback to EC on their specific operation experience with the systems previously designed, in the cases that EC gets awarded a revamp or an expansion of the existing system and the same individuals are part of the organization of the new project. Otherwise only biased informal feedback is provided by chance or through developed relations.

Formal operations feedback, when provided, does not include as specific feedback as (i) hazards which were overlooked or incorrectly assessed as unlikely or not serious, (ii) potential failures or design errors not included in the hazard analysis nor (iii) identified hazards inappropriately accepted rather than being fixed. What is usually reported are ineffective design controls, which is articulated as operability issues (e.g. perception of how easy or difficult a system is operated) and maintenance problems (e.g. having to replace components more often than expected). The point is that there is never such a detailed analysis by EC, clients or operators addressing the points listed above unless a serious incident occurs. Probably the reason is that this type of work is not easy to get funded because organizations do not see a fast return of investment.

3.2.3.1.2Feasibility of Step Implementation in EC and By-Products

The need for development of knowledge about operations is recognized in EC. It is expected that implementation will be feasible. On the other hand, involvement of clients' operations units (when available) is expected to be more difficult and highly dependent on specific project organizations and their readiness (awareness) to spend resources on this.

3.2.3.1.3Development of Step for the Project Example

In this Project Example, EC's direct client Design Institute and its client as well as investor and most likely future operator of the pipeline system, have provided poor input regarding available experience. Most of the time, they have referred to Russian norms and standards and have instructed EC to gather information from that literature. Russian norms and standards are, however, more prescriptive than illustrative of the experience which has triggered establishing them. Since the intent ofDesign Institute with this contract was to try to find better solutions to be compared with the solutions of the previous Investment Justification, their general strategy has been one way learning from EC rather than sharing. This might have also been influenced by schedule constraints, which have again played a decisive role (as in many other projects) not allowing for open discussions on lessons learned, for example.

The high-level operations constraints listed in Table 15 above have been identified by analysis of available experience mainly related to (i) general pipeline systems operations, (ii) port operations and (iii) specific multiproduct transport operations. This available experience has been elicited from experts in EC and from the body of knowledge of the Oil & Gas industry.

3.2.3.1.4Definition of High-Level Guidelines for Implementation of Step in EC

A practicable way to introduce this step in EC and to generally improve the knowledge about operations is to systematically perform lessons learned workshops at the start of the project together with client. These sessions should facilitate open sharing of experiences rather than a one way communication, even if clients expect a deliverable from EC, as it is usual. Also the documentation generated should be comprehensive and precise. Both parties should be aware of the bilateral benefits. This way the costs could be assigned to the specific projects and the project management teams could see a short-term return in the frame of the projects. A central analysis group should collect the results of the lessons learned workshops and analyse them. Prerequisite for this must be open, comprehensive and precise documentation of experiences in the workshops, otherwise it is very difficult to generate usable conclusions beyond high-level guidelines, which anyways can be found in general literature.

Another way of developing knowledge about operations in EC would be to prepare case studies about the commissioning of systems. This should be performed mainly during the commissioning activities. It is recognized that this might be difficult again due to the time pressure normally faced during commissioning, especially if numerous problems are experienced. But this is probably the only practicable way due to the fact that once an assignment is finalized, teams are demobilized as soon as possible and assigned to other projects, therefore not having time anymore for reflection.

EC should promote involvement of operations units in all hazard analyses to be performed, if not possible in the related workshops, at least by review of related documentation.

3.2.3.2 Delivering Safety Requirements and Constraints to Operations

3.2.3.2.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 79 to 86. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting “Delivering safety requirements and constraints to operations” in column “Element of Using STAMP”.

The safety information delivered to operations is usually communicated in (i) operation and maintenance concepts, manuals and procedures depending on the project phase in which the engineering work is performed and (ii) operator training, where the operation and maintenance procedures are introduced to the operator's personnel. In the operation and maintenance manuals, safety-related points are marked as such; and during the operator training, those points are highlighted as safety-related and the risks involved are explained.

The level of detail of the safety information delivered to operations basically depends on (i) the existence and degree of involvement of an operations group in the client organization —most pipeline projects are developed by joint ventures which often do not have an operations unit established and also have different opinions on operational matters— and (ii) the project phase.

Table 27 summarizes what and how the safety information is passed to operations.

Safety Information	**Passed to Operations?**	**In which project phase?**	**Where in the documentation?**
Operational Assumptions	Yes, however not always marked as safety-related and as assumptions.	All, however marked as safety-related and as assumptions usually during "Execute" (Commissioning and Handover to Operations).	Sometimes in Basis of Design. Eventually in Operation and Maintenance Manual.
Safety Constraints	Yes, however not always marked as safety-related.	All, however marked as safety-related and as assumptions usually during "Execute" (Commissioning and Handover to Operations).	Sometimes in Basis of Design and HAZID/HAZOP Close-out Reports. Eventually in Operation and Maintenance Manual.
Safety-related Design Features	Yes, however not always marked as safety-related.	Detail Design during "Execute".	Sometimes in a List of SCE (Safety Critical Elements), however this is usually limited to Safety Instrumented Functions. Otherwise in the related specifications.

Safety Information	**Passed to Operations?**	**In which project phase?**	**Where in the documentation?**
Operating Assumptions	Yes, however not always marked as safety-related and as assumptions.	All, however marked as safety-related and as assumptions usually during “Execute” (Commissioning and Handover to Operations).	Sometimes in Basis of Design. Eventually in Operation and Maintenance Manual.
Safety-related Operational Limitations	Yes, however not always marked as safety-related and as limitations (depending on project phase).	All, however marked as safety-related and as limitation usually during “Execute” (Commissioning and Handover to Operations).	Sometimes in Basis of Design. Eventually in Operation and Maintenance Manual.
Training and Operating Instructions	Yes	“Execute” (Operator Training and Commissioning)	Operation and Maintenance Manual
Audits and Performance Assessment Requirements	No, operators define requirements afterwards themselves.	-	-
Operational Procedures	Yes	Operational concepts at end of “Define”. Operational Procedures in “Execute” (Commissioning and Handover to Operations).	Operational concepts in Operation and Maintenance Philosophy. Operational Procedures in Operation and Maintenance Manual.
Safety Verification and Analysis Results	No, such activities are usually not required or clients perform them by themselves through audits.	-	-

Table 27: Safety Information passed to Operations

The rationale behind why a piece of safety information is identified as such is generally weak so that traceability between project phases and between organizations involved is difficult. There seems to be a culture of minimum documentation so that often only the individuals directly involved in the hazards analyses and the preparation of Basis of

Design and specifications precisely know why a certain requirement or constraint is safety-related and why it has been defined. Interviewees have different opinions about how easy traceability of information is. This shows that traceability is possible, however not straightforward (as opposed to the pointers system of an intent specification).

Operators are generally not aware about the value of the safety information created during development for running an operations safety control structure. The findings illustrated in Table 27 are not only specific to EC practice, but as already pointed in other sections, are driven by client requirements, therefore probably specific to the Oil & Gas industry in general. This shows that, for example, audits and performance assessment requirements are not requested by clients, therefore showing that clients and operators are not aware of the importance of design safety information for those. This is of vital importance for pipeline projects developed by joint ventures, as introduced above, because these projects do not have operational structures in place when design is developed, so the operations safety control structure has to be created from scratch. For projects where an operations unit is strong (e.g. expansion of existing pipeline systems) and an operations safety control structure is in place, it is interesting to note that awareness is greater, but there seems to be an overreliance on the established systems so that again attention to ensure communication of safety information generated during development seems to be lacking.

Interviewees generally associate identification of Safety-Critical Elements (SCE) and definition of maintenance priority with performing SIL Assessments.

3.2.3.2.2Feasibility of Step Implementation in EC and By-Products

According to Table 27, operational assumptions, safety constraints, safety-related design features, operating assumptions and safety-related operational limitations are not consistently passed to operations in all project phases but only at the end of "Execute" as part of operation and maintenance manuals. This is most probably because this safety information is not readily available at the end of the previous project phases.

The established practice in EC and the potential for implementation of STAMP Elements related to these pieces of safety information have been addressed in the sections above in 3.2.2 "Engineering Development". If an intent specification approach is adopted, then passing the safety information generated during development to operations is reduced to a matter of (i) raising client's awareness and (ii) agreeing to recognize this step as a project task during contract negotiations. This is so because once an intent specification approach is established, traceability of information of any kind is straightforward. Therefore it is noted that the feasibility of implementation of this step depends greatly on the success of implementation of steps in Engineering Development.

Training and operating instructions as well as operational procedures are prepared and passed to operations, as long as this task is included in the scope of contracts. Audits and performance assessment requirements as well as safety verification and analysis results are elements of safety information which seem to be managed by clients and operators themselves, when there is an established operations unit in the organization.

3.2.3.2.3Development of Step for the Project Example

The sections above in 3.2.2 "Engineering Development" provide examples of the type of information to be produced and how to connect the different bits with pointers. The following tables provide references to the tables above.

Safety Information	**Reference to Examples provided in Tables (3.2.2 "Engineering Development")**
Operational Assumptions	Some in Table 11 and Table 13
Safety Constraints	- Safety Constraints in Table 7 - High-level Operation Constraints in Table 15 - Lower Level Operation Requirements and Design Constraints in Table 18
Safety-related Design Features	Table 19
Operating Assumptions	Some in Table 11 and Table 13
Safety-related Operational Limitations	Table 26

Table 28: References to Examples of Safety Information (to be passed to Operations) for the Komsomolsk – De-Kastri Project

Examples for (i) training and operating instructions, (ii) operational procedures, (iii) audits and performance assessment requirements as well as (iv) safety verification and analysis results have not been developed for the Project Example because these are not part of the scope of work for the current project phase.

3.2.3.2.4Definition of High-Level Guidelines for Implementation of Step in EC

As indicated above, the guidelines for implementation of STAMP Steps in 3.2.2 "Engineering Development" should be adopted first of all for having the safety information generated during design development available. After that strategies should be developed in order to (i) raise client's awareness about the value of safety information and (ii) agree to recognize this step as a project task during contract negotiations.

3.2.4 Management

3.2.4.1 Providing Leadership for Safety Matters

3.2.4.1.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 87 to 96. The worksheet is in **Error! Reference source**

not found.. The findings can be filtered by selecting “Providing leadership for safety matters” in column “Element of Using STAMP”.

Participation of Project Managers in safety-related activities seems to be common. Most of them refer to their participation in hazard analysis activities such as HAZIDs, HAZOPs and SILs and in ensuring close-out of recommendations proposed. Depending on the specific project organization, some Project Managers and/or Engineering Managers also participate in preparing and approving safety-related design philosophies and design solutions. Business Unit Directors generally do not participate directly in project specific safety-related activities, but believe they are confronted with safety-related issues on a weekly basis.

Comments provided in answers to other parts of the Initial Status Review show that:

- The general impression is that the Oil & Gas industry is more hazardous than others, but for example not as hazardous as the Nuclear Power Industry to which some interviewees have explicitly referred.
- Performing hazard analysis such as HAZIDs, HAZOPs and SILs is considered costly and Project Managers wish to have alternative tools (e.g. standard safety-related design philosophies) which could reduce the durations of these sessions.
- The impression is that safer systems cost more (e.g. specifying SIL 3 components which are not manufactured by many suppliers, providing extra containment means for the event of hydrocarbon spills, over sizing fire water systems so that they could deal with catastrophic scenarios, etc.)

It is generally believed that accidents can be prevented, but this can only be achieved by a good design together with good operation practices.

The review could not interview EC employees (not managers) as to find out what their impression was regarding leadership provided by managers for safety-related matters. Two Business Unit Directors reported about issuing communications on safety matters to their teams. The impression of the Author is that EC employees believe that managers care the most about productivity (time and cost spent in project activities).

3.2.4.1.2Feasibility of Step Implementation in EC and By-Products

As reported by Leveson, commitment and leadership by management has been identified as the most important factor for creating a strong Safety Culture in organizations. Leadership creates Culture and Culture drives Behavior. Therefore it is considered necessary to implement this step.

Improving commitment and leadership by management including Management Directors, Business Unit Directors and Project/ Engineering Managers is considered necessary and feasible. Changing the perception that safety is expensive and emphasizing the positive by-products of designing for safety as proposed by Leveson are key points for development of leadership.

3.2.4.1.3Definition of High-Level Guidelines for Implementation of Step in EC

A series of discussion panels between Managing Directors, Business Unit Directors and Project/ Engineering Managers should be performed. A panel is not training, but a discussion between participants. This way they can arrive at their own conclusions and realize on their own about the returns of investing in safety. After managers have come to conclusions, they should propose actions to demonstrate their commitment to the rest of employees. One of these sessions could be performed in the yearly EC Group Management Conference. A quarterly panel of one to two hours sessions is considered sufficient to ensure creative thinking and efficiency.

Top management should issue communications on safety matters. For example one communication channel could be the EC Group Newsletter “EC News”.

3.2.4.2 Implementing a Safety Policy

3.2.4.2.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 97 to 105. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting “Implementing a safety policy” in column “Element of Using STAMP”.

The Safety Policy of EC is included in the HSE Commitment of the EC Group as shown in Figure 14. No other policy documents have been found.

The review showed that managers consider the existing Safety Policy (i) a very high-level policy and (ii) an occupational health and safety oriented policy (i.e. a policy focused on protecting individuals during the course of the engineering services provided by EC) as opposed to a policy on how to design systems for safety. Project Managers point that the existing Safety Policy cannot be used in projects. It is also recognized that the existing Safety Policy does not provide guidance on decisions when safety conflicts with other goals. Interviewees reported that conflicts are solved on a case by case basis. Some interviewees pointed that the fact of not having a developed and comprehensive Safety Policy with the aim of designing systems for safety does not help solving conflicts and contributes to costly internal and external discussions where finding consensus is difficult because there is no basis on which to argue. This has been identified as having a very significant impact on project progress and claim management results.

The review team reported unanimously that project schedules do not allow for delays due to safety concerns. Some also reported that project schedules do not even foresee the time necessary for performing hazard analysis.

Employees are aware about the existing Safety Policy, but as explained, this policy is not the type of policy they can use in their daily design work.

3.2.4.2.2Feasibility of Step Implementation in EC and By-Products

Leveson proposes the Safety Policy should be broken in two parts. The first being a short and concise statement of the safety values and what is expected from employees with respect to safety; the second being a set of documents detailing how the policy is to be implemented.

It is considered necessary (as repeatedly mentioned by the review team) and feasible to gradually develop a Safety Policy on designing systems for safety.

Figure 14: HSE Commitment EC Group [4] -deleted

3.2.4.2.3Definition of High-Level Guidelines for Implementation of Step in EC

In a first stage of step of implementation the existing HSE Commitment of the EC Group (concise statement of the safety values and what is expected from employees with respect to safety) should be amended to explicitly addressing at least:

- Organization’s safety goals as to how to design systems for safety
- Organization’s priorities as to how to solve conflicts between (design) safety and other organizational goals

A second stage of step implementation would develop the set of documents detailing how the policy is to be implemented including the safety-related design philosophies as described in several steps above.

As the new Safety Policy on designing systems for safety is gradually developed, awareness can be gradually raised, for example by distributing Safety Alerts with articles and incident reports or by editing a safety column in the EC Group Newsletter “EC News”, an interviewee proposed.

Top management commitment should be provided in a similar fashion as it has been recently provided for establishing the new Compliance Management Process in EC. This process focuses on assurance of (i) social responsibility, (ii) quality of services provided, (iii) integrity, (iv) objectivity, (v) fairness and (vi) prevention of corruption and it has the foremost attention of top management.

3.2.4.3 Implementing a Safety Management Plan

3.2.4.3.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 106 to 108. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting “Implementing a safety management plan” in column “Element of Using STAMP”.

Project specific development safety management plans are prepared as part of project set-up only if clients require it. If prepared, these are typically a part of an overall HSE Plan. The emphasis of those HSE Plans, especially in the “Execute” phase, is on assuring occupational health and safety rather than design for safety. This has also been observed in the analysis of 3.2.4.2 “Implementing a Safety Policy”.

Although not completely surveyed, it can be stated that management (Project Managers and Business Unit Managers) do not think project specific development safety management plans are always necessary, and often believe those are an administrative burden rather than a tool for facilitation of management. This suggests that these plans are rarely operationalized and there is a need for improvement of those.

Table 29 summarizes the elements of project specific development safety management plans usually addressed when EC prepares those.

Elements of Project Development Safety Management Plan	**Addressed?**	**Operationalized?**

Elements of Project Development Safety Management Plan	**Addressed?**	**Operationalized?**
Scope and objectives, applicable standards, documentation and reports.	Yes	Yes, listed standards are used and contract deliverables are prepared.
Safety Organization: Roles and responsibilities, coordination, system safety interfaces with other groups.	Yes	Partly, defined roles and responsibilities are fulfilled depending on available resources. The same applies to interface management arrangements. Also highly dependent on the priority client assigns to compliance with specified organizational arrangements.
Procedures: Hazard and risk analysis, safety-driven design, management of change, training, decision-making and conflict resolution.	Only if explicitly required by client. If so, partly, there are never procedures for safety-driven design and decision-making and conflict resolution.	Partly. The culture seems to be of minimum documentation, managers try to save resources and this has an impact on the quality of procedures implementation.
Schedule of Safety Activities: Milestones, checkpoints, timing of activities, reviews and required participants.	Usually only list of activities. If a detailed proposal has been previously prepared, then yes.	Yes
Safety Information System: Hazard and risk analysis, hazard logs, hazard tracking and reporting systems and applicable lessons learned.	Partly, lessons learned are not included.	Partly. The culture seems to be of minimum documentation, managers try to save resources. There is no awareness about the importance of safety information beyond the project phase in which EC has been contracted.

Table 29: Elements of Project specific Development Safety Management Plans usually addressed

While the discussion above has been limited to project specific development safety management plans, it is recognised that a similar analysis should be performed at the EC operational level, i.e. is there an EC specific management plan for assurance of designing for safety? The next section 3.2.4.4 “Implementing a Safety Control Structure” analyses some of the elements, mainly safety organization.

3.2.4.3.2Feasibility of Step Implementation in EC and By-Products

A project specific development safety management plan is the result of a planning effort. This project specific planning effort starts during proposal preparation (a task which ends delivering a cost estimate for that part of scope) and continues during project set-up, in the event of contract award. Planning efforts can be made more agile by the use of standards (e.g. standards for procedures in hazard and risk analysis, safety-driven design, management of change, training, decision-making and conflict resolution) which should be part of implementing a Safety Policy. It is necessary and feasible to improve planning efforts for assuring safety in design. This has been recognized by EC top management.

3.2.4.3.3Definition of High-Level Guidelines for Implementation of Step in EC

As introduced above, a project specific development safety management plan should be started as part of proposal preparation, this should include:

- Proposal for Project Design for Safety (or the terminology client specifies in tender) in text including
  - Scope and objectives, applicable standards and deliverables,
  - Safety organization (roles and responsibilities, coordination, system safety interfaces with other groups),
  - Applicable procedures (hazard and risk analysis, safety-driven design, management of change, training, decision-making and conflict resolution),
  - Description of safety activities and
  - Description of safety information system (hazard and risk analysis, hazard logs, hazard tracking and reporting systems and applicable lessons learned).
- Project Plan in MS Project or similar including
  - Schedule of safety activities (milestones, checkpoints, timing of activities, reviews and required participants),
  - Resources (capacities and hourly rates) according to safety organization described in the text proposal.

In case of contract award, the plan should be transposed into a project document and revised in case of changes.

Strategies for ensuring operationalization of plans should be developed, for example by development of standards for all the elements of project development safety management plans, and in general by implementing the suggestions of this thesis.

3.2.4.4 Implementing a Safety Control Structure

3.2.4.4.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 109 to 121. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting “Implementing a safety control structure” in column “Element of Using STAMP”.

At the time of performing the Initial Status Review there was no visible group in EC responsible for safety in the projects. Individuals from different Business Units (GB-M Pipeline Systems, GB-S Process Facilities, GB-I Instrumentation, Automation and Telecom) have been performing safety activities guided by their respective Business Unit Managers and Project Managers. Very recently a Safety Group has been created collecting individuals from GB-M and GB-S and placed in a department of GB-S, which has now been renamed to “Process Engineering and Safety”. Nevertheless the findings of the Initial Status Review regarding implementation of a safety control structure remain valid, as this is a very recent structural change.

Managers generally believe that the safety efforts performed have an impact in the designs EC produces, but often too late. They also recognize that safety efforts are not part of mainstream system engineering in the projects.

Safety-related design decisions are by no means taken independently of Project Managers (who are usually governed by cost, schedule and mission accomplishment goals). In EC, Project Managers have an engineering background and often are also Engineering Managers; this is a deliberate policy in EC in order to ensure that project management decisions are not taken independently from engineering. While this policy does have a point, it is arguable because at the same time independence is reduced. This is confirmed by the fact that the Safety Group does not enjoy the prestige (and independence) necessary to have influence on decision making that safety requires. As remarked, Project Managers are the ultimate authority in projects.

The designated safety working group at a corporate level (different than the recently created so-called Safety Group which is mainly a pool of resources for safety activities in projects) is the Virtual Competence Team for Technical Safety. As reported below in 3.2.4.5 “Implementing a Safety Information System”, knowledge transfer between projects and different EC companies is facilitated by this initiative but the problem of those is that they are not project driven (costs cannot be allocated to specific projects, and eventually be transferred to clients). Therefore these initiatives are rather slow and their development relies greatly on the individuals managing the teams.

EC currently does not implement corporate development safety standards. This has been remarked in all parts of this thesis. Management of change is not implemented systematically (see also 3.2.4.3 “Implementing a Safety Management Plan”).

Sufficient resources for safety-related activities are not available and this is an issue already identified by management. It is believed that most of employees performing safety-critical activities do not have the appropriate skills, knowledge and resources for that. Lack of operations experience and certificates of competence have been highlighted as key issues for improvement.

Employees performing safety-related decisions are rarely fully informed and sometimes not skilled. As reported above, safety efforts are not part of mainstream system engineering and there is a lot of work to be done for improving awareness and competence of employees not part of the new so-called Safety Group.

The quality and level of comprehensiveness of the hazard analysis performed depends greatly on the (i) clients' requirements, (ii) project managers' awareness about importance of exercises and (iii) designated chairmen (for the hazards analyses developed in workshops).

As reported above, it is generally believed that results of hazard analysis are usually considered when safety-related decisions are to be made, but not in a systematic way.

3.2.4.4.2Feasibility of Step Implementation in EC and By-Products

A safety control structure is both necessary in the projects and in EC. The EC part of the project safety control structure is controlled by the EC corporate safety control structure. The figure below illustrates this. The red parts of this simplified Safety Control Structure are the typical Project Safety Control Structure EC is part of.

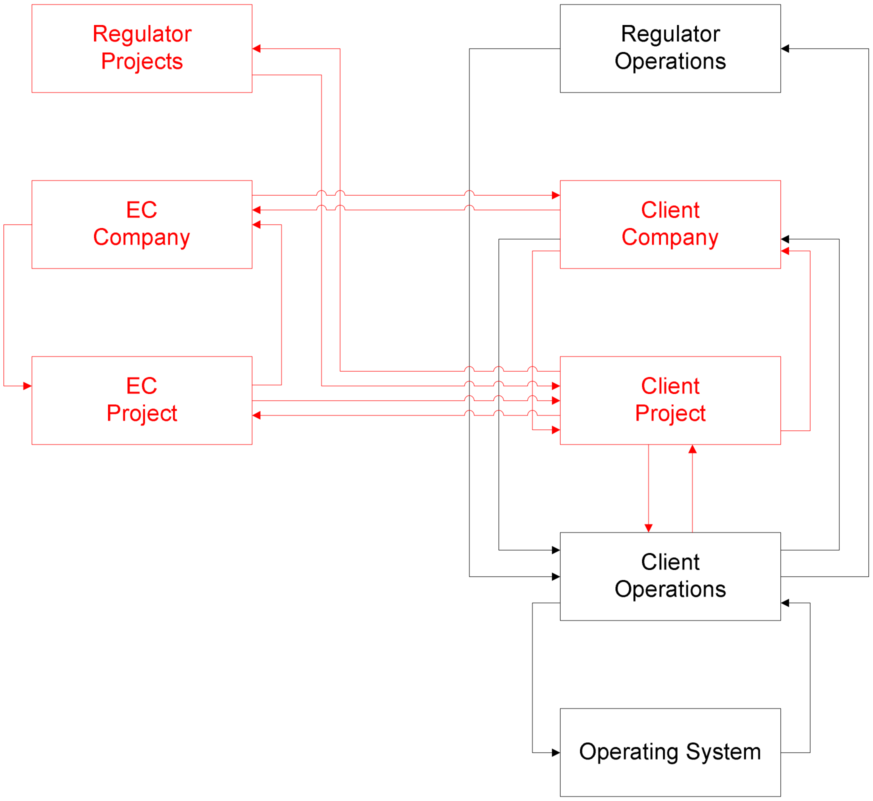


Figure 15: Simplified Typical Safety Control Structure for EC projects (based on Fig. 4.4. of [1]).

The first step towards establishing the EC Safety Control Structure has been recently made creating the "Safety Group" in the department "Process Engineering and Safety". This is a fundamental step which will be further supported by management, otherwise it is not possible to implement any improvements for integration of safety in system engineering.

3.2.4.4.3Definition of High-Level Guidelines for Implementation of Step in EC

As already indicated, a “Safety Group” in the department “Process Engineering and Safety” has been recently created. This is a first step towards establishing the EC Safety Control Structure and a deliberate decision to include this discipline in an engineering group, not in an assurance group. The visibility of the “Safety Group” has been improved (see Figure 16 below), but its independence in the projects has not.

Figure 16: Organization Chart of EC Company, Status July 2012 [23] -deleted

Leveson reports that organizations successfully operating high-risk technologies have a major characteristic in common, namely that they place a premium on safety and reliability by structuring their programs so that technical and safety engineering organizations own the process of determining, maintaining, and waiving technical requirements with a voice that is equal to yet independent of Program Managers, who are governed by cost, schedule, and mission accomplishment goals. Policies for independence of the "Safety Group" need to be developed.

Another key measure is to define responsibilities for personnel performing safety-critical activities and decisions. This includes definition of safety-related responsibilities of project team members which are not part of the "Safety Group" (e.g. project managers, engineering managers, other discipline engineers). The list of responsibilities provided in "Engineering a Safer World" Chapter 13.2.6 should be used as guidance. Further responsibilities for implementation of STAMP in EC are also listed in the next section 3.3 "Strategy for Integrating Safety into EC's System Engineering process".

All this will accompany the development of the Safety Policy.

3.2.4.5 Implementing a Safety Information System

3.2.4.5.1Current EC Practice

The findings documented herein mainly result from the analysis of answers to Initial Status Review questions no. 122 to 124. The worksheet is in **Error! Reference source not found.**. The findings can be filtered by selecting "Implementing a safety information system" in column "Element of Using STAMP".

Management (Project Managers and Business Unit Managers) does not think a safety information management system as such is necessary. Managers generally believe that established document management systems are sufficient for that. Table 30 summarizes the elements of a project safety information management system usually implemented by EC.

Elements of Project Safety Information Management System	**Implemented?**	**Where in the documentation?**
Development Safety Management Plan	Sometimes, if required by client. See also 3.2.4.3 "Implementing a Safety Management Plan"	Project set-up documentation.
Status of safety-related activities	Rarely systematically documented. If there is a nominated Design Safety Manager (in EC called Technical Safety Manager) in the project, then the knowledge about status is with him/her. If not, then with the Project Manager or Engineering Manager.	Sometimes in project weekly and monthly reports, when required by client. Sometimes in action tracking systems, again if required by client.

Elements of Project Safety Information Management System	**Implemented?**	**Where in the documentation?**
Safety constraints and assumptions underlying the design, including operational limitations	Not systematically and not marked as safety-related, as reported above in 3.2.2 "Engineering Development".	Sometimes in Basis of Design and hazard analysis reports. Eventually in Operation and Maintenance Manual.
Results of hazard analysis (hazard logs) and assessments	Yes. If a hazard analysis is performed, then a report is normally prepared including so-called worksheets which are developed in the workshops (e.g. HAZID, HAZOP, SIL).	Hazard analysis reports.
Tracking and status information on all known hazards	Not systematically. Not centralized.	Close-out reports of individual lists of recommendations/ actions issued by hazard analyses (e.g. HAZID, HAZOP, SIL).
Lessons learned and historical information	No. See also 3.2.3.1 "Considering Relevant Operations Experience in the Development"	-

Table 30: Elements of Project Safety Information Management System usually implemented

Communication of safety information between project phases depends almost completely on the policy of clients, since they are the stakeholders collecting the information generated during design and passing it to another organization for example for further design, construction or operation. In general, traceability of safety information between project phases and between organizations involved is difficult.

There is no effective communication of safety information between projects and between EC Companies. The EC Group is running a Knowledge Portal (internet based document management and sharing platform) and Virtual Competence Teams for different disciplines. Knowledge transfer between projects and different EC companies is facilitated by these initiatives. The problem of those, however, is that they are not project driven (costs cannot be allocated to specific projects, and eventually be transferred to clients). Therefore these initiatives are rather slow and again their development relies greatly on the individuals managing the teams.

3.2.4.5.2Feasibility of Step Implementation in EC and By-Products

Regarding the feasibility of implementation of a safety information management system for single projects, improvements will rely mainly on nominated Design Safety Managers (in EC called Technical Safety Managers). This should be feasible because the safety information management systems support their activities. This will hopefully also bring improvement to the management of safety information between project phases, although the control here is at the clients' side.

Regarding the feasibility of implementation of a safety information management system between projects, as introduced above, the Knowledge Portal and Virtual Competence Teams initiatives exist and need to be further supported by top management.

3.2.4.5.3Definition of High-Level Guidelines for Implementation of Step in EC

The main measure for implementation of a project safety information management system is connected to implementing a project specific development safety management plan as described in 3.2.4.3 "Implementing a Safety Management Plan". This should be a first stage of implementation.

A second stage of implementation based on availability of project information would be the implementation of a corporate safety information management system. The Knowledge Portal and Virtual Competence Teams initiatives would need to be further supported by top management so that resources are made available. This relates also to the measures described in 3.2.3.1 "Considering Relevant Operations Experience in the Development" which would contribute to this further development.

3.3 Strategy for Integrating Safety into EC's System Engineering process

The following requirements for implementation of STAMP principles in EC have been developed in the previous section 3 "Application of STAMP to Integration of Safety into System Engineering"; details on implementation and the rationale behind can be found there. The same structure is used in this chapter for facilitation of traceability.

Two stages of implementation have been defined:

- First Stage of Implementation: these are measures which can be implemented right away without need of additional resources.
- Second Stage of Implementation: these are measures which cannot be implemented right away because development requires additional resources which have to be made available by EC Managing Directors.

3.3.1 First Stage of Implementation

The following measures are applicable to all project phases, unless otherwise stated.

3.3.1.1 Measures for Establishing the Goals of the System

Measure	**Responsible**
Agree on high-level system (functional and non-functional) goals as part of contract negotiations.	Project Manager Acquisition
Ensure high-level system (functional and non-functional) goals are documented as part of contract.	Project Manager Acquisition

Measure	**Responsible**
If high-level system (functional and non-functional) goals cannot be documented as part of contract, ensure they get documented in the Basis of Design.	Project Manager or Engineering Manager
If a design is inherited, ensure high-level system goals (functional and non-functional) are documented along with the inherited design constraints (analyzed during the Design Review process) in the Basis of Design.	Project Manager or Engineering Manager

Table 31: First Stage Measures for implementing "Establishing the Goals of the System"

3.3.1.2 Measures for Defining Accidents

Measure	**Responsible**
Develop a typical set of unacceptable losses.	Safety Group
Develop a General Risk Matrix Criteria [plausibility x unacceptable losses].	Safety Group
If a client does not provide own Risk Criteria, discuss the General Risk Matrix Criteria and agree on unacceptable losses as part of contract negotiations.	Project Manager Acquisition
Ensure unacceptable losses are documented as part of contract.	Project Manager Acquisition
If unacceptable losses cannot be documented as part of contract, ensure they get documented in the Basis of Design.	Project Manager or Engineering Manager

Table 32: First Stage Measures for implementing "Defining Accidents"

3.3.1.3 Measures for Identifying System Hazards

Measure	**Responsible**
Develop a typical set of high-level system hazards.	Safety Group
Discuss the typical set of high-level system hazards with client (during kick-off meeting) and agree on a small set applicable to the project.	Project Manager or Engineering Manager
Ensure high-level system hazards get documented in the Basis of Design.	Project Manager or Engineering Manager

Table 33: First Stage Measures for implementing "Identifying System Hazards"

3.3.1.4 Measures for Integrating Safety into Architecture Selection and System Trade Studies

These measures are applicable only to Conceptual Design (Facility Lifecycle Phase "Select").

Measure	**Responsible**
Discuss identified high-level system hazards for comparison of pre-selected options (in a small workshop). **Remark:** This is a more simple type of exercise than the one to be performed as part of second stage implementation, see below 3.3.2.4, which will first aid acceptance of the exercise.	Project Manager or Engineering Manager
Ensure discussion of identified high-level system hazards for comparison of pre-selected options is documented as part of typically System Selection Study.	Project Manager or Engineering Manager

Table 34: First Stage Measures for implementing "Integrating Safety into Architecture Selection and System Trade Studies"

3.3.1.5 Measures for Documenting Environmental Assumptions

Measure	**Responsible**
Ensure discipline leaders list assumptions when they write their inputs to Basis of Design.	Project Manager or Engineering Manager
Ensure assumptions get documented in the Basis of Design (in the form of a List of Assumptions, see Table 12).	Project Manager or Engineering Manager
Review the Project List of Assumptions in design review meetings.	Project Manager or Engineering Manager
Verify validity of assumptions in the Project List of Assumptions during internal gate reviews meetings.	Project Manager or Engineering Manager
Ensure assumptions get precisely documented in the hazard analyses performed.	Safety Group
Transpose assumptions made in hazard analyses performed to the Project List of Assumptions.	Project Manager or Engineering Manager

Table 35: First Stage Measures for implementing "Documenting Environmental Assumptions"

3.3.1.6 Measures for Generating System-Level Requirements

No first stage measures have been defined for implementing “Generating System-Level Requirements”. The matter needs to go through a standardization of Basis of Design, which is a longer term measure.

3.3.1.7 Measures for Identifying High-Level Design and Safety Constraints

No first stage measures have been defined for implementing “Identifying High-Level Design and Safety Constraints”. The matter needs to go through a standardization of Basis of Design, which is a longer term measure.

3.3.1.8 Measures for Performing System Design and Analysis

Measure	**Responsible**
Agree on Project Safety-related Activities as part of contract negotiations.	Project Manager Acquisition
Ensure Project Safety-related Activities are documented as part of contract.	Project Manager Acquisition
Expand the scope of traditional hazard analyses techniques (HAZID and HAZOP) for introduction of STPA (Systems-Theoretic Process Analysis) elements, i.e. introducing guidewords/ deviations on enforcement of safety constraints. **Remark:** Do not increase duration of workshops while expanding the scope.	Safety Group

Table 36: First Stage Measures for implementing “Performing System Design and Analysis”

3.3.1.9 Measures for Documenting System Limitations

Measure	**Responsible**
Ensure limitations get documented in the Basis of Design, starting with limitations related to basic functional requirements and to assumptions, in the form of a List of Limitations.	Project Manager or Engineering Manager
Incorporate in the Project List of Limitations the limitations related to hazards not controlled and to trade-offs during internal gate reviews meetings.	Project Manager or Engineering Manager
Ensure limitations get precisely documented in the hazard analyses performed.	Safety Group

Table 37: First Stage Measures for implementing “Documenting System Limitations”

3.3.1.10 Measures for Considering relevant Operations Experience in the Development

Measure	Responsible
Perform Lessons Learned workshops at the start of the project together with client.	Project Manager or Engineering Manager
Promote involvement of operations units in all hazard analyses to be performed. If not possible in the related workshops, at least by review of related documentation.	Project Manager or Engineering Manager

Table 38: First Stage Measures for implementing “Considering relevant Operations Experience in the Development”

3.3.1.11 Measures for Delivering Safety Requirements and Constraints to Operations

No specific first stage measures have been defined for implementing “Delivering Safety Requirements and Constraints to Operations” since it is considered that the first stage measures for the Engineering Development steps need to be established first so that safety information is readily available before passing it to operations.

3.3.1.12 Measures for Providing Leadership for Safety Matters

Measure	Responsible
Plan a series of discussion panels between Managing Directors, Business Unit Directors and Project/ Engineering Managers on the topic of investing in safety.	Managing Directors
Propose actions for demonstrating commitment to providing leadership for safety matters.	Managing Directors
Edit a column on “Designing for Safety” in the EC Group Newsletter “EC News”	Managing Directors

Table 39: First Stage Measures for implementing “Providing Leadership for Safety Matters”

3.3.1.13 Measures for Implementing a Safety Policy

Measure	Responsible
Revise the existing HSE Commitment of the EC Group to explicitly address at least: - EC’s safety goals as to how to design systems for safety - EC’s priorities as to how to solve conflicts between (design) safety and other organizational goals	Managing Directors

Table 40: First Stage Measures for “Implementing a Safety Policy”

3.3.1.14 Measures for Implementing a Safety Management Plan

Measure	**Responsible**
Start a Project specific Development Safety Management Plan as part of proposal preparation.	Project Manager Acquisition
In case of contract award, revise the Project specific Development Safety Management Plan into a separate project document.	Project Manager or Engineering Manager

Table 41: First Stage Measures for "Implementing a Safety Management Plan"

3.3.1.15 Measures for Implementing a Safety Control Structure

The following measures can be started right away and need to be continued during second stage implementation together with the further development of the Safety Policy.

Measure	**Responsible**
Define responsibilities for personnel performing safety-critical activities and decisions.	Safety Group
Define policies for developing independence of the "Safety Group".	Managing Directors, Safety Group

Table 42: First Stage Measures for "Implementing a Safety Control Structure"

3.3.1.16 Measures for Implementing a Safety Information System

The first stage measures should focus on implementing a Safety Information System within a project. No specific first stage measures have been defined for "Implementing a Safety Information System" since the first stage measures for "Implementing a Safety Management Plan" implicitly include those —see elements of a Safety Management Plan in Table 29.

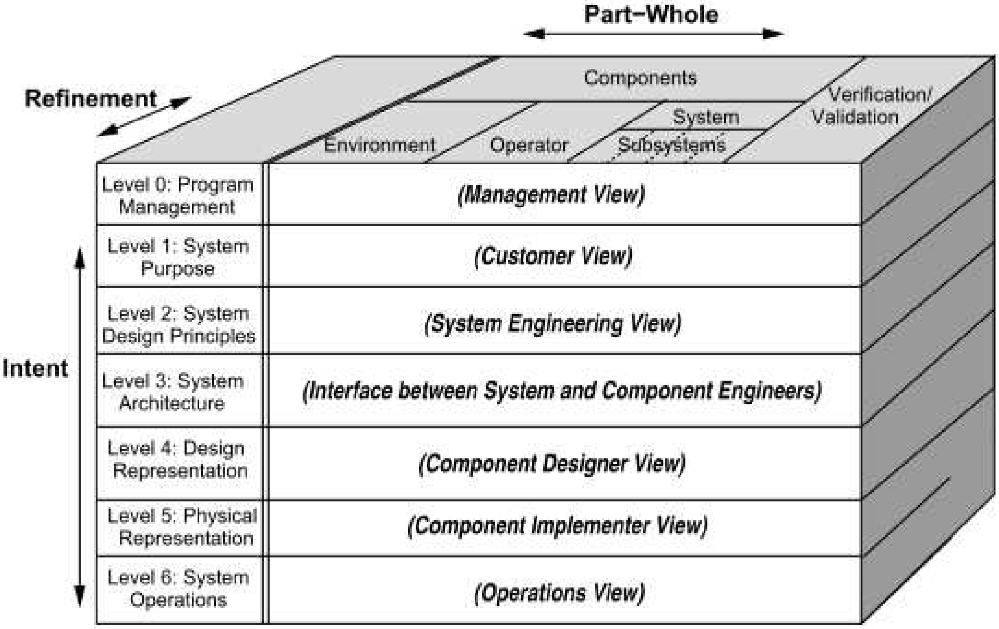
3.3.2 Second Stage of Implementation

Three fundamental measures have been defined for the second stage implementation:

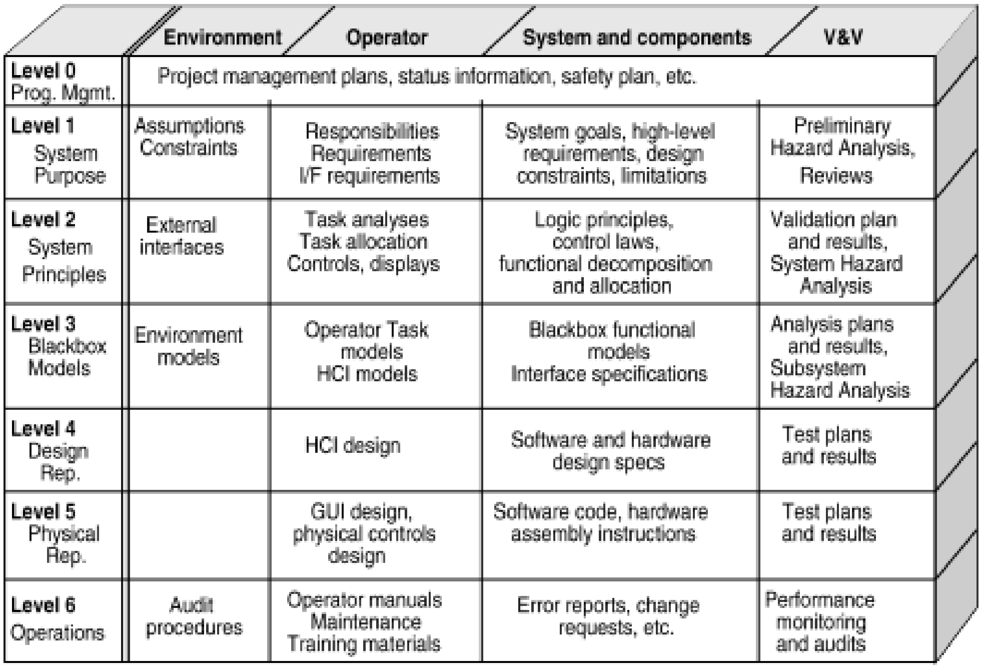
- Development of EC Safety Policy
- Standardization of:
  - Safety-related Design Philosophies

    To be based on international good practice (analysis of available regulations, norms and standards). Once these EC standard safety-related design philosophies have been prepared, they should be further analysed for improvement by performing STPA Analysis (an example for this has been provided in 3.2.2.8 "Performing System Design and Analysis").
  - Project Development Safety Management Plans.

- Discussion and agreement on the purpose and scope of Basis of Design in projects, and standardization of preparation of Basis of Design following the intent specification approach proposed by Leveson (see Figure 6 and Figure 7 above, hereunder reproduced again to facilitate reading)


Part–Whole
Refinement
Components
Environment
Operator
System
Subsystems
Verification/ Validation
Intent
Level 0: Program Management
(Management View)
Level 1: System Purpose
(Customer View)
Level 2: System Design Principles
(System Engineering View)
Level 3: System Architecture
(Interface between System and Component Engineers)
Level 4: Design Representation
(Component Designer View)
Level 5: Physical Representation
(Component Implementer View)
Level 6: System Operations
(Operations View)

The Structure of an Intent Specification [1]



	Environment	Operator	System and components	V&V
Level 0 Prog. Mgmt.	Project management plans, status information, safety plan, etc.			
Level 1 System Purpose	Assumptions Constraints	Responsibilities Requirements I/F requirements	System goals, high-level requirements, design constraints, limitations	Preliminary Hazard Analysis, Reviews
Level 2 System Principles	External interfaces	Task analyses Task allocation Controls, displays	Logic principles, control laws, functional decomposition and allocation	Validation plan and results, System Hazard Analysis
Level 3 Blackbox Models	Environment models	Operator Task models HCI models	Blackbox functional models Interface specifications	Analysis plans and results, Subsystem Hazard Analysis
Level 4 Design Rep.		HCI design	Software and hardware design specs	Test plans and results
Level 5 Physical Rep.		GUI design, physical controls design	Software code, hardware assembly instructions	Test plans and results
Level 6 Operations	Audit procedures	Operator manuals Maintenance Training materials	Error reports, change requests, etc.	Performance monitoring and audits

An Example of the Information in an Intent Specification [1]

3.3.2.1 Measures for Establishing the Goals of the System

Measure	**Responsible**
Develop guidelines for agreement and clear documentation of high-level system goals (functional and non-functional) as part of contract negotiations.	Managing Directors
If client does not provide own safety-related design philosophies, discuss and agree on safety-related design philosophies as part of contract negotiations. **Pre-requisite:** standard safety-related design philosophies have been developed.	Project Manager Acquisition

Table 43: Second Stage specific Measures for "Establishing the Goals of the System"

3.3.2.2 Measures for Defining Accidents

No specific second stage measures have been defined for implementing "Defining Accidents". Unacceptable losses would be considered in the development of safety-related philosophies as part of STPA Analysis, as introduced above.

3.3.2.3 Measures for Identifying System Hazards

No specific second stage measures have been defined for implementing "Identifying System Hazards". Documentation of identified high-level system hazards should follow the guidelines to be developed as part of standardization of Basis of Design.

3.3.2.4 Measures for Integrating Safety into Architecture Selection and System Trade Studies

These measures are applicable only to Conceptual Design (Facility Lifecycle Phase "Select").

Measure	**Responsible**
Analyse identified high-level system hazards for comparison of pre-selected options (in a workshop) using the agreed project Risk Matrix Criteria. **Remark:** This is a more formal type of exercise than the one to be performed as part of first stage implementation, see above 3.3.1.4.	Project Manager or Engineering Manager

Table 44: Second Stage specific Measures for implementing "Integrating Safety into Architecture Selection and System Trade Studies"

3.3.2.5 Measures for Documenting Environmental Assumptions

No specific second stage measures have been defined for implementing "Documenting Environmental Assumptions". Standardization of Basis of Design should establish the guidelines for documenting environmental assumptions as part of Basis of Design.

3.3.2.6 Measures for Generating System-Level Requirements

No specific second stage measures have been defined for implementing "Generating System-Level Requirements". Standard design philosophies (safety-related and non-safety related will define typical system-level requirements for the types of systems EC designs. Standardization of Basis of Design should establish the guidelines for documenting system-level requirements as part of Basis of Design.

3.3.2.7 Measures for Identifying High-Level Design and Safety Constraints

Standard design philosophies will define typical high-level design and safety constraints for the types of systems EC designs. Standardization of Basis of Design should establish the guidelines for documenting high-level design and safety constraints as part of Basis of Design.

Measure	Responsible
Transpose the findings and recommendations of studies normally performed by EC in the Conceptual Design phase into the Project Basis of Design. **Remark:** This should be gradually implemented for single studies (i.e. a chapter of Basis of Design) in different projects. Eventually a standard for those could be generated too. This is only applicable to Conceptual Design (Facility Lifecycle Phase "Select").	Project Manager or Engineering Manager

Table 45: Second Stage specific Measures for implementing "Integrating Safety into Architecture Selection and System Trade Studies"

3.3.2.8 Measures for Performing System Design and Analysis

Measure	Responsible
Develop standard operation and control philosophies as well as specifications of safety-critical systems with the aid of STPA	Safety Group
Develop a policy to define the level of detail that operation and control philosophies and specifications of safety-critical systems should contain.	Managing Directors, Safety Group

Table 46: Second Stage specific Measures for implementing "Performing System Design and Analysis"

3.3.2.9 Measures for Documenting System Limitations

No specific second stage measures have been defined for implementing "Documenting System Limitations". Standardization of Basis of Design should establish the guidelines for documenting system limitations as part of Basis of Design.

3.3.2.10 Measures for Considering relevant Operations Experience in the Development

Measure	Responsible
Develop a process for analysis of results generated in lessons learned workshops in the frame of the Knowledge Portal and Virtual Competence Teams initiaves. The results should be included in the Corporate Safety Information Management System, see Table 51 below.	Managing Directors
Develop a process for preparation of case studies about the commissioning of systems.	Managing Directors

Table 47: Second Stage specific Measures for implementing "Considering relevant Operations Experience in the Development"

3.3.2.11 Measures for Delivering Safety Requirements and Constraints to Operations

Measure	Responsible
Develop strategies for raising clients' awareness about the value of safety information.	Managing Directors
Agree with clients to recognize the work involved in "Delivering Safety Requirements and Constraints to Operations" as a project task during contract negotiations.	Managing Directors

Table 48: Second Stage specific Measures for implementing "Delivering Safety Requirements and Constraints to Operations"

3.3.2.12 Measures for Providing Leadership for Safety Matters

No specific second stage measures have been defined for implementing "Providing Leadership for Safety Matters". These should be developed in the frame of discussions as indicated above in Table 39.

3.3.2.13 Measures for Implementing a Safety Policy

Measure	Responsible
Develop a set of documents detailing how the safety policy is to be implemented.	Managing Directors

Table 49: Second Stage specific Measures for "Implementing a Safety Policy"

3.3.2.14 Measures for Implementing a Safety Management Plan

Measure	Responsible
Develop strategies for ensuring operationalization of Project specific Development Safety Management Plans.	Managing Directors

Measure	**Responsible**
Develop standards for preparation of Project specific Development Safety Management Plans.	Managing Directors

Table 50: Second Stage specific Measures for “Implementing a Safety Management Plan”

3.3.2.15 Measures for Implementing a Safety Control Structure

The measures started during first stage implementation, as listed in Table 42, need to be continued during second stage together with the further development of the Safety Policy.

3.3.2.16 Measures for Implementing a Safety Information System

Measure	**Responsible**
Develop a Corporate Safety Information Management System in the frame of the Knowledge Portal and Virtual Competence Teams initiaves.	Managing Directors

Table 51: Second Stage specific Measures for “Implementing a Safety Information System”

4 Conclusions

The use of STAMP (System-Theoretic Accident Model and Processes) and the guidelines given in Leveson’s “Engineering a Safer World” provide a comprehensive, detailed and useful frame for evaluating how an organization designs for safety (or not). This is often not the case when trying to perform such an exercise with industry safety assurance standards because they are too general. By reviewing the current EC practice against Leveson’s guidelines, specific problems have been identified and measures tailored to EC have been proposed.

The feasibility of implementing STAMP and STPA (System-Theoretic Process Analysis) principles in EC relies greatly on applying the new techniques for standardization of design philosophies. This matches the identified need for development of a comprehensive Corporate EC Safety Policy (i.e. a policy on how to design systems for safety) and a Safety Control Structure that shall ensure the policy gets implemented. This will require an important standardization effort. Besides these major measures to be inevitably performed, there are a lot of less resource demanding measures that can be implemented right away, especially during the initial stages of a project (namely project proposal preparation, contract negotiations and project set-up) and still have a very significant impact on how safety is designed into the system.

STPA is a powerful tool for generating comprehensive and precise requirements in the design of safety-critical (and most probably not safety-critical) systems. While it is not considered practicable to depart in the short term from the traditional hazard analysis techniques (HAZID, HAZOP, SIL, QRA) because those techniques are very rooted in the Oil & Gas industry practice, it is considered feasible to expand the scope of HAZID and HAZOP to include elements of STPA. This will be further investigated.

With the implementation of STAMP and STPA principles not only the safety of the engineered systems can be improved, but also the efficiency of engineering management activities and the quality of the engineering work delivered. Implementing an Intent Specification approach for the preparation and revision of Basis of Design through the different project phases will solve a lot of the typical engineering management problems of major capital projects, i.e. traceability, interface management, documentation of usually undocumented assumptions and limitations, etc.

5 Outlook

The immediate next steps are to implement the First Stage Measures proposed in this thesis and obtain resources for implementation of the Second Stage Measures for:

- Development of EC Safety Policy;
- Standardization and improvement of Safety-related Design Philosophies with the aid of STPA (System-Theoretic Process Analysis);
- Standardization of Project Development Safety Management Plans;
- Discussion and agreement on the purpose and scope of Basis of Design in projects, and standardization of Basis of Design following the principles of an Intent Specification.

The implementation of the proposed measures should be direct input to the further development of the EC Basic Design Workflow, which is in development since May 2011 and is part of the EC Corporate Project Management System, soon to be made a standard.

The potential of the new techniques goes beyond the limited definition of Safety in this thesis as absence of fatalities and injuries during system operation. This means it is possible to use the principles of STAMP (System-Theoretic Accident Model and Processes) and STPA for engineering of system to avoid any type of unacceptable losses such as, for example, the following identified for the Komsomolsk – De-Kastri Multiproduct Pipeline Project studied:

- A.1 "*Oil Products cannot be transported and delivered*";
- A.2 *"Oil Product tankers' schedules disrupted"*; or
- A.3 *"Quality of Oil Products delivered deviates from specification"*.

Moreover, the potential for transferring STAMP and STPA principles to other related fields should be subject of further study and would most probably bring improvement, e.g.:

- Project Risk Management (i.e. engineering a project control system to avoid schedule slippages and budget overrun);
- Corporate Management (i.e. development or improvement of management systems).

References

[1] Leveson, N. G., 2011. Engineering a Safer World. Systems Thinking Applied to Safety. MIT Press, Engineering Systems Series. ISBN 978-0-262-01662-9, Jan 2012.

[2] -deleted

[3] IEC 61511-3. Functional Safety – Safety Instrumented Systems for the Process Industry Sector. Part 3: Guidance for the determination of the required Safety Integrity Levels. Ed. 1.0 2003-03.

[4] -deleted

[5] Trans Balkan Pipeline, 2012. Website. Available from http://www.tbpipeline.com/ [Accessed 15 March 2012]

[6] DEEP, KBB, EKB, E.ON, IVG, JadweBay, OMV, Statoil, VNG, 2011. Cavern Storage Etzel. Securing Supplies of Natural Gas and Oil. Available from http://www.jade-bay.de/ [Accessed 15 March 2012]

[7] Gasunie, 2010. Gasunie to tackle Security of Supply Bottlenecks. Available from http://www.gasunie.nl/ [Accessed 15 March 2012]

[8] Gasunie, 2011. Projektinfo Quarnstedt. Available from http://www.erdgas-fuer-morgen.de/ [Accessed 15 March 2012]

[9] Gasunie, 2011. Einwohnerversammlung Quarnstedt Neubau Verdichterstation. Available from http://www.erdgas-fuer-morgen.de/ [Accessed 15 March 2012]

[10] -deleted

[11] -deleted

[12] -deleted

[13] -deleted

[14] -deleted

[15] ISO, 2000. ISO 17776 “Petroleum and natural gas industries —Offshore production installations— Guidelines on tools and techniques for hazard identification and risk assessment”. ISO 17776:2000(E)

[16] -deleted

[17] -deleted

[18] -deleted

[19] -deleted

[20] -deleted

[21] Fleming, C, Leveson, N.G., Spencer, M., (Massachusetts Institute of Technology), Wilkinson, C. (Honeywell Aerospace Advanced Technology, Columbia, Maryland). Safety Assurance in NextGen. NASA. NASA/CR-2012-217553, March 2012.

[22] Thomas, J., 2012. Extending and Automating STPA for Requirements Generation and Analysis. Presentation in 1st STAMP/STPA Workshop 18.04.2012.

[23] -deleted

Appendix 1 Initial Status Review Checklist

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
1	Development	All	Level 1	Establishing the goals of the system	10.2 10.3 10.3.1	Are system goals usually agreed between EC and client?	Yes. Typical system goals include: (i) system (pipeline) throughput (functional goal), expansion steps (functional goal), sometimes properties of fluids to be processed (functional goal), technology and design shall be state of the art (quality goal), in compliance with aplicable regulations, norms and standards (quality goal).	Yes and documented in the contract.	Yes. Typically system throughput, system availability and system lifetime are quantified goals the new system has to fullfil becoming contractual terms for EC.	Functional goals yes. Safety-related goals are not agreed and those vary from client to client and from country to country.	System goals were known to EC from previous phases (Appraise and Feasibility phases where EC had also been involved).	Yes and documented in the contract. However safety-related standards were not available. The client (IOC-13 and IOC-14) did not have developed any safety-related standards and the previous FEED work did not define those either. EC had to develop all safety-related philosophies from scratch.	Systems' goals were clear in the contracts for different stations (Compressor Station Quarnstedt, Compressor Station Achim, Metering Station Ellund, Metering Station Heidenau). The IOS Frame Agreement established the overall IOS Portfolio goals.	Functional goals were clear. IOC-1 provided basis data (transport scenarios in terms of pressures and volumes). Norms and standards as per Austrian law had to be complied with (but this is known for any project). IOC-1 does not have any design philosophies documented, but we have worked with IOC-1 for many years, we know how they work/ what they want and they know how we work.
2	Development	All	Level 1	Establishing the goals of the system	10.2 10.3 10.3.1 7.3	Is formal documentation of system goals usually practiced? If so, where in the project documentation?	Yes, as part of contract or as part of documents to be issued at the begining of the project such as basis of design or design manual.							
3	Development	All	Level 1	Establishing the goals of the system	10.2 10.3 10.3.1 7.3	How clearly are the system goals articulated?	In most of the contracts system goals are clearly articulated, however in some not. Especially in contracts with "unexperienced" clients definition of goals is not clear. EC normally recognises this from the begining of relations with client, but still accepts this situation due to strategical business decisions.	Some are quantified such as (for Gas Storages) Throughput, Inlet and Outlet Pressures, Switching Times, Dew Points, Availability. Others are not so clearly written, typically "developing a design in compliance with applicable, laws, norms, regulations and standards".	See 1. System throughput, availability and lifetime are usually articulated quantitatively and are documented in contracts and Basis of Design. Other type of goals (e.g. regarding compliance with safety or environmental standards) are expressed in a more difuse way.	Functional goals are clearly articulated. Other goals not. Scope of work are generally not clearly formulated. Different clients understand different things out of the same scope of work in contracts (e.g. IOC-7). This is because those are often not specific enough. Making standards part of contracts would definetely help. For example people have different understanding of what is meant by hydrotest, leak test and service test. Also Double Block and Bleed (DBB) is generally not understood. Standards for Isolation Philosophies, Manual Venting and Manual Draining Philosophies need to be developed so that we all understand the same. Also in order to be more efficient in our work.	System goals were clearly written in the Project contract (i.e. Initial System Throughput 35 MTA to be expanded to 50 MTA, Availability, Lifetime, Minimization of Environmental Impact).	Functional goals were clearly articulated. The EPCM JV (Detail Engineering Contractor with EC, EC as silent consortium partner) had to contractually fullfil a "Process Guarantee" on system goals.	Systems' goals were clearly written (e.g. operation points, inlet and outlet pressures, maximum velocity, maximum temperature, volume (Nm3/h), etc.)	Functional goals were clearly articulated.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
4	Development	All	Level 1	Establishing the goals of the system	10.2 10.3 10.3.1 7.3	Are inherited constraints (i.e. decisions taken by others which EC must adhere to in order to pursue a project) formally documented as such along with the system goals?	Not always. In 25% of contracts (subjective estimate) constraints are not visible (identified) at the begining of projects or are wrongly defined by client (e.g. for pipeline system typically routing and definition of locations for facilities have been approved in a previous phase, and it turns being not optimal or not feasible)	If we inherit a design from another organisation whatever documentation available is part of the contract. Also it is required as per EC's Integrated Management System to perform a Design Review. Inherited constraints are then identified in the course of the review. In some cases EC has to contractually fullfil a "Process Guarantee" on system goals, therefore it is of vital importance to review what the previous organisation has decided.	EC recommended practice suggests to perform a Design Review of any design inherited. This is not always performed because it is a task normally not payed by clients. Inherited constraints get documented in Design Review reports and Basis of Design.	GB-U does not perform design yet, but PMC (Project Management Consulting) reviews of designs by others. Whatever information is made available is reviewed.	Even if EC had performed the studies work in the previous phase (Feasibility) it was difficult to find and use previous information. Feasibility took place in 2001 and different people had been involved. For example the previous Site Selection Study was poorly documented in the Feasibility phase which implied having to perform a comprehensive Site Selection Study before starting the Basic Design. Therefore the Site Selection constraints had to be re-identified.	The previous FEED work had also been performed by EC. However during the FEED development the client wished a higher level of detail than the design EC was producing (every client has a different understanding of how detailed a Basic Design and FEED should be). Eventually the FEED was accepted but in the Detail Design (part of the EPCM) the client requested EC to review the FEED accordingly. This took about 4 months. The substance of the FEED did not change though, so in practical terms the inherited constraints were confirmed and further detailed for the EPCM phase.	For CS Quarnstedt, MS Ellund and CS Achim, Concept Selection and Functional Design was previously performed by EC. Information was available however due to changes in contracts with Shippers, operation points changed so that the Functional Designs had to be changed before starting with Basic Design. Basic Design for MS Heidenau was performed by Basic Engineering Contractor. Documentation was provided by IOC-16. EC's scope of work was Detail Design for that station.	IOC-1 awarded the complete engineering services to EC form concept selection to commissioning. IOC-1 provided basis data which including data about exisiting facilties which had to be verified by EC. For example the loop lines followed the same route as the existing pipeline (that was not something subject of discussion). Also there was restricted space available in the existing compressor stations (Baumgarten).
5	Development	All	Level 1	Establishing the goals of the system	10.2 10.3 10.3.1	If EC's contract scope does not require to start the system engineering process from scratch but to continue on the basis of the work previously performed by a different organisation, do you think it is a sensible practice to still formally agree and document system goals before starting the work? If so, do you usually find system goals documented in the work previously performed by a different organisation which the EC can refer to?	Yes, it must be performed. It is usually part of contract and documentation already existing or it is documented at the begining of the project in basis of design or design manual.	See 4. In the frame of design reviews the system goals are reviewed.	See 4. In the frame of design reviews the system goals are reviewed.	Yes, it is sensible. Not always, depends on the project.	System goals were clearly written in the Project contract, even if the Project had already undergone Feasibility ca. 7 years before.	Yes, it is sensible. Not always, depends on the project.	For the MS Heidenau, EC soon identified that the tie-in points were not adequate and the safety distances and overall the layout in the Basic Design inherited were too small. The client wanted to use a space left available at the location, which was too reduced. Such constraints were not accepted by EC and were communicated to the client which implied having to redo the Basic Design by EC before being able to carry on with Detail Design.	EC performed a verification of the data about the exisitng facilties.
6	Development	All	Level 1	Defining accidents and unacceptable losses	7.1	What do you understand as accident?	Accident may be a loss of life or injuries (loss of workforce), loss of production, loss or damage of assets.							
7	Development	All	Level 1	Defining accidents and unacceptable losses	7.1	What do you understand as unacceptable loss?	Any loss is unacceptable.							
8	Development	All	Level 1	Defining accidents and unacceptable losses	7.1	What do you think clients understand as accidents and/or unacceptable losses?	Clients understand the same (Accident may be a loss of life or injuries (loss of workforce), loss of production, loss or damage of assets. Any loss is unacceptable).							

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
9	Development	All	Level 1	Defining accidents and unacceptable losses	10.2 10.3 10.3.2	Are accidents and unacceptable losses usually defined as such and documented in the project? If so, where in the project documentation?	Sometimes yes, normally indirectly in the form of reference to regulations, norms and standards, sometimes not. If so, not in one specific piece of documentation for such, but disseminated over many documents and not in a consistent way.	Accidents and unacceptable losses are usually defined in client's Standards. Some clients do not have such standards though, in that case and usually only if a risk assessment has to be performed, EC proposes Risk Criteria.	Accidents and unacceptable losses are usually defined in client's Standards for HSE Risk Criteria in terms of impacts to Human Health&Safety, Environment, Assets and Client's Reputation, however as part of a so-called Risk Matrix which also takes proabability into consideration (e.g. IOC-2, IOC-6, IOC-3/ IOC-4). Some clients do not have such standards though, in that case and usually only if a risk assessment has to be performed, EC proposes Risk Criteria calibrating another client's Standard which has been found to work well in the past and is found adequate for the project/client of matter.	Not always, it is very client and country related. If so, in related policies.	Pipeline companies for new developments are usually created from scratch and do not have developed and agreed standards as opposed to other operators. IOC-5 Company did not have defined accidents and unacceptable losses. Those were not part of contractual documentation, but developed prior to start of Risk Assessments and documented in the related reports.	A Safety Layer Matrix (IEC 61511-3) was proposed by the client and reviewed during the HAZOP before the SIL Assessment was performed.	IOC-16 proposed a Risk Graph (IEC 61511-3) before performing the SIL Assessment. However this was re-calibrated by Gasunie together with EC and Certification Party (LP: independent 3rd. Party certification) before it was used. That was a wish by IOC-16 management which found criticality assigned to loss of assets was not adequate and wished to change it. A Project Risk Assessment was performed by IOC-16 Netherlands and had a different Risk Criteria.	A Risk Graph (IEC 61511-3) was proposed by EC for calibration before the HAZOP and SIL Assessment. Otherwise not.
10	Development	All	Level 1	Defining accidents and unacceptable losses	7.1 10.2 10.3 10.3.2	How are accidents and unacceptable losses identified (specified)?	Normally as part of contract or applicable regulations, norms and standards.							
11	Development	All	Level 1	Defining accidents and unacceptable losses	7.1 10.2 10.3 10.3.2	Are accidents and unacceptable losses agreed between client and other stakeholders?	Yes, as part of contract.	Yes. See 9.	Yes. See 9.	See 9.	Accidents and unacceptable losses were agreed and defined between EC and client after begining of the Project, since IOC-5 Company did not have those defined.	Yes. See 9.	In this Project IOC-16 management changed their Risk Graph (IEC 61511-3) standard because 500 k€ commercial loss had been considered a Great impact but they considered that did not reflect their opinion).	See 9.
12	Development	All	Level 1	Defining accidents and unacceptable losses	7.1 10.2 10.3 10.3.2	Do you think EC's industry has defined those?	Yes.	Yes. Typically LOC.	Generally yes, but clients define those too as part of their corporate HSE Policy. See 9.	Yes, western clients usually provide such a policy, Russian or Chinese clients somehow try to define/adopt such policies but their implementation very often is not supported within the organizations.	Generally yes, but they needed to be defined specifically for the Project.	Yes. Also IEC 61511-3.	See 11.	Yes. IEC 61511-3. Although the ranges on commercial impact have to be carefully agreed with client.
13	Development	All	Level 1	Defining accidents and unacceptable losses	7.1 10.2 10.3 10.3.2	What are common accidents and unacceptable losses?	Typically fire and explosion events, but there are very different acceptability criteria in the industry for those (i.e. different operators have different criteria).	Typically fire and explosion events, but there are very different acceptability criteria in the industry for those (i.e. different operators have different criteria). For example IOC-8 Risk Matrix does not consider the so-called "Low Probability High Impact Events" as acceptable, others do.	It depends on how Safety is defined. Nowadays Risk Criteria are defined not only in terms of Health&Safety, but some include losses regarding Environment, Assets, Reputation or Production.	Typically LOC, Fire and Explosions.	To me it is not completely clear where Safety starts and where it ends (the boundaries of Safety). For the Project losses were mainly defined as fire and explosion events, oil spills as well as loss of assets.	Typically LOC, Fire and Explosions.	Fire and Explosion. Acceptable/ unacceptable losses according to client's policy.	Typically LOC, Fire and Explosions.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
14	Development	All	Level 1	Defining accidents and unacceptable losses	7.1 10.2 10.3 10.3.2	When do you think accidents and unacceptable losses should be agreed/defined in a project?	At the begining of projects and documented as part of contract.	Before a Risk Assesment is performed. Clients ususally do not bother much about defining Risk Criteria as long as no Risk Assessment has to be performed.	If client has a Standard for HSE Risk Criteria (see 9), then this is defined at the begining of the project because such standard together with others are part of the contract. However they will probably be "used" later in the project when a Risk Assesment is planned to be performed. In my opinion, accidents and unacceptable losses should be defined at the begining of the project however the latest before performing a Risk Assesment (e.g. HAZOP and SIL Assessment).	From the begining, as standard part of the contract, otherwise we are on permanent re-engineering (e.g. DBB - Double Block and Bleed- very often discussed).	Not discussed in interview. Answer by Business Area 1 is considered representative.	From the begining, as standard part of the contract. If such standards don't exist, then Ideally the during the kick off meeting. In this Project, the Risk Criteria (as also other safety-related policies and philosphies) was not defined and it had to be developed when it was needed.	The Risk Graph (IEC 61511-3) was calibrated before performing the SIL Assessment.	Not discussed in interview.
15	Development	All	Level 1	Defining accidents and unacceptable losses	7.1 10.2 10.3 10.3.2	If EC's contract scope does not require to start the system engineering process from scratch but to continue on the basis of the work previously performed by a different organisation, do you think it is a sensible practice to still formally agree and document the accidents and unacceptable losses which should be avoided? If so, do you usually find accidents and unacceptable losses documented in the work previously performed by a different organisation which EC can refer to?	Yes, it must be performed. It is usually part of contract and documentation already existing. However sometimes there is no documentation to refer to and definition of accidents or unacceptable losses is also not performed by EC.							
16	Development	All	Level 1	Identifying system hazards	7.2	What do you understand as hazard? (NGL: Why do accidents/ hazards occur?)	A threat which might lead to an accident.							
17	Development	All	Level 1	Identifying system hazards	7.2	Do you think component failures are hazards? (NGL: What is the major cause of hazards?, What role do failures have in hazards?)	Component failures can be hazards, but not necessarily, depending on the component and on the back-ups and safety measures.	Not discussed in interview.	Component failures are not necessarily hazards. Recently a so-called SPF (Single Point of Failure) Review for IOC-10 was performed. IOC-10 owns a gas plant producing fuel gas which feeds a power plant. The intent of the SPF Review was to identify which component failures might lead to unacceptable loss of production. 7 SPFs were identified, however only 1 of 7 was identified also having impact on Safety (also leading to an accident as traditionally defined). 6 of 7 SPFs would "only" lead to ESD (Emergency Shut Down) with no further implications for Humans, Environment or Assets.	Any component possibly subject to LOC is a hazard basically (e.g. pipe welds, HP/LP interfaces). Component failures are potential sources of hazards, especially if those components are part of safety-critical systems. For example if a LOC occurs, ESD system and containment shall be available. A failure of those can lead to massive fire and explosions. However every year there are numerous LOC (e.g. gas clouds) which disperse with no further implications.	Not discussed in interview.	Not necessarily. A component failure might or might not be a hazard. It has to be analysed.	Not always. If there are adequate safety instrumented functions implemented, then the system can be kept in a fail safe state (e.g. fire and gas detection system fails, then the unit is isolated and depressurized and ventilation ducts are closed so that no flammable concentrations are formed).	Component failures can be hazards, especially the failure of a Safety Critical System, that's why we perform SIL Assessments.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
18	Development	All	Level 1	Identifying system hazards	7.2.2 10.3.3	Does EC usually identify high-level system hazards?	Yes, but not systematically.	Through HAZID (actually in Basic Design).	Not discussed in interview. Answer by Business Area 1 is considered representative.	If a safety issue is evident during the Concept Selection phase, then those are discussed in general meetings. In Basic Design and Detail Design through HAZIDs.	System hazards were identified by Environmental Consultant in a HAZID which was part of the HSE tasks they were subcontracted.	In this Project through the HAZID.	System hazards were identified in HAZIDs.	Not in this Project.
19	Development	All	Level 1	Identifying system hazards	7.2.2 10.3.3	When do you think high-level system hazards should be identified in a project?	At the very begining.	As early as possible, however HAZID can only be performed with a certain level of design maturity (i.e. PFDs, process description, meteo data, seismic data, preliminary layout, etc.)	Not discussed in interview. Answer by Business Area 1 is considered representative.	As early as possible.	System hazards were identified relatively early in the Project in a HAZID workshop using the Bow-Tie methodology. This was lead by Environmental Consultant.	As early as possible.	HAZIDs were performed on PFDs and preliminary layout.	Not discussed in interview.
20	Development	All	Level 1	Identifying system hazards	7.2.2	Do you think it makes sense to derive high-level system hazards from specific component hazardous behavior (i.e. bottom-up process)?	No sense.	Not discussed in interview.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview.	Some component failures (e.g. equipment, piping, fittings, gauges, operator error) were identified as threats in the HAZID workshop potentially leading to LOC (Loss Of Containtment).	Not discussed in interview.	Not discussed in interview.	Not discussed in interview.
21	Development	All	Level 1	Identifying system hazards	7.2.2 10.3.3	When EC performs high-level system hazards identification, how are high-level system hazards usually identified?	High-level hazards are identified by experienced individuals in the frame of initial project meetings.	In a HAZID workshop with Project team members and sometimes with client.	Not discussed in interview. Answer by Business Area 1 is considered representative.	See 18.	Hazards were identified in a HAZID workshop using Bow-Tie methodology.	For this Project in the HAZID aided by a checklist.	See 18.	In HAZID aided by a checklist.
22	Development	All	Level 1	Identifying system hazards	7.2.2 10.3.3	When EC performs high-level system hazards identification, are domain experts involved in indentifying high-level system hazards?	Yes. High-level hazards are identified by experienced individuals in the frame of initial project meetings.							
23	Development	All	Level 1	Identifying system hazards	7.2.2 10.3.3	When EC performs high-level system hazards identification, are (agreed/defined) accidents and unacceptable losses considered when identifying high-level system hazards?	Yes, but not systematically.	Only if the HAZID also requires a Risk Analysis.	Not discussed in interview. Answer by Business Area 1 is considered representative.	That would surely be helpful so that we do not need to be constantly re-designing (e.g. requirement for DBB Double Block and Bleed valves or not?)	The only accident considered in the HAZID workshop was Loss Of Containment. Possible causes (the barriers in place preventing those happening) and the potential consequnces were identified.	Not in this Project. Risk Criteria was developed later for SIL Assessment.	The HAZIDs were developed aided by a typical checklist.	Usually not.
24	Development	All	Level 1	Identifying system hazards	7.2.2 10.3.3	When EC performs high-level system hazards identification, do you think EC's industry has defined standard hazards which should always be addressed?	Yes, some (e.g. loss of containment, fire and explosion)	Yes, checklists.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Typically LOC, Fire and Explosions.	In this Project and many others Loss Of Containment is the Top Event addressed. However the only consequences which were identified as a losses in this exercise were (i) Major Unignited Spill affecting onsite, offsite, sea, land and (ii) Major environmental impact as a result of release from above ground/below ground pipeline.	Yes, typical checklist.	Yes, typical checklist.	Typically LOC, Fire and Explosions.
25	Development	All	Level 1	Identifying system hazards	7.2.2 10.3.3	When EC performs high-level system hazards identification, how detailed are the hazard registers produced? Are they large lists?	There are no hazard registers produced at that point.	Yes, they can be large lists and tracking of actions is sometimes tedious.	Not discussed in interview. Answer by Business Area 1 is considered representative.	HAZID Registers can be quite long. However other registers which are of even more cruciality like HP/LP Interface Register, SRD Register, LO/LC Register are not used/developed in EC at all.	In total 18 Bow-Ties were produced in the HAZID workshop where the losses to prevent would have been as written in 24. A lot of barriers preventing threats to develop into LOC were identified.	A HAZID Register was prepared and the actions are followed-up. Yes.	The typical checklist is rather detailed so that registers generated were of 20 to 50 lines.	HAZID Registers can be quite long.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
26	Development	All	Level 1	Identifying system hazards	7.3 10.3.3 10.3.7	Are high-level requirements and design constraints identified/specified along with the identified high-level system hazards?	No.							
27	Development	All	Level 1	Identifying system hazards	7.3 10.3.3 10.3.7	Do you understand these high-level requirements and design constraints are somehow anyways specified in industry/client standards, which are then usually considered by domain expert engineers when preparing project specific safety-related design philosophies? If so, do you think this is sufficient?	Yes. To a great extent systematically. Not sufficient, a project specific approach is always necessary.	For gas storage projects the clients always provide safety philosophies which we have to consider when designing. If the client does not provide those, EC engineers propose applicable best practice. The recommendations of HAZID and also HAZOP are followed-up and closed. If there are actions related to philosophies for the next Project phase, then these have to be considered, but this is not performed systematically.	Yes, client standards are good and are used by system experts to prepare design philosophies. If client does not have own standards then the system experts propose relevant best practice.	Safety-related requirements vary greatly from client to client or even from country to country. The western approach seems far more developed than the Russian or Chinese approach. See 12. In any case whatever project specific safety-related philosophies foreseen are included in the Basis of Design.	In this Project the results of this HAZID were not considered when preparing safety-related philosophies.	There were no safety-related standards available, so philosphies had to be first prepared considering good practice and then further developed/ detailed as the different hazard analysis were performed (HAZID, HAZOP, SIL, QRA).	Yes, DVWG, ATEX, Gasunie TSP engineering standards, EON Ruhrgas standards provide guideline for safety-related design. Also Dutch norms have been used where German norms were either not available or not adequate. Where standard specifications from either IOC-16 or IOC-8 and IOC-17 (previous gas grid owners) were not adequate EC has prepared those (filter separators, coolers,etc.) and performed a Gap Analysis.	IOC-1 did not have design philosophies documented. EC worked according to good practice and previous experience with IOC-1 also for the WAG system. What is prepared in Austria is a so-called Projekthandbuch (Project Manual) which is actually a high-level basic design which already includes PFDs and layouts. This is a document to be submitted to authorities for permitting.
28	Development	All	Level 1	Identifying system hazards	7.3 10.3.3 10.3.7	What PHA techniques do you find adequate for deriving high-level requirements and design constraints?	Brainstorming with experts.	Not discussed in interview.	Not discussed in interview. Answer by Business Area 1 is considered representative.	HAZID.	Not discussed in interview.	All techniques we used in the Project are valuable. HAZID delivers more high-level recommendations.	Not discussed in interview.	Not discussed in interview.
29	Development	All	Level 1	Identifying system hazards	7.2.2 10.3.3	If EC's contract scope does not require to start the system engineering process from scratch but to continue on the basis of the work previously performed by a different organisation, do you think it is a sensible practice to still identify high-level system hazards which should be controlled? If so, do you usually find available hazard registers in the work previously performed by a different organisation which EC can refer to?	Yes, it should be performed. If the contract is to perform Concept Selection or Basic Design, normally not. If the contract is to perofrm Detail Design, normally there is a HAZOP Report available, but not always a hazard register.	Not discussed in interview.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Yes. Not always.	Previous Hazard Registers as such were not readily available. See 4.	Yes, in the Project we performed HAZID. There was no hazard registers available from the previous FEED (also performed by EC). Maybe a coarse HAZOP had been performed but no safety-related philosophy was developed with their results. We developed all hazard analysis new from scratch.	Not discussed in interview.	Not discussed in interview.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
30	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	Does EC usually consider high-level hazards (safety) when selecting an overall system architecture between feasible options (a.k.a. system optimization, system selection or concept selection)?	Yes somehow, but never systematically.	What is usually done is a very high-level hazard identification and then options to be compared are proposed so that those hazards are avoided.	Not discussed in interview. Answer by Business Area 1 is considered representative.	For process plants it is not easy to consider safety for concept selection unless very evident issues are identified. Normally there is not enough information available when deciding between options to evaluate safety.	In this Project even if the HAZID results did not find their way into the design development, EC's practice and the prominency of the ESIA study to be performed for the Greek and Bulgarian government managed that pipeline route and locations for SPMs (Single Point Mooring), Pump Stations and Tank Farms were studied considering Safety and Enviromental concerns.	Not applicable in this project.	Not in this project. Functional requirements combined with CAPEX/OPEX estimations were used. Reciprocating machines were excluded because in order to comply with the required compression more than 3 machines had to be installed. Centrifugal compressors with E-drive would have required a high voltage supply nearby which was not available. Turbine driven compressors were left as the only sensible option. On the other hand it is known that common leaks during normal operation are larger for Centrifugal Compressors than for Reciprocating Compressors.	No. In our domain concept selection is a rather simple matter, it is about deciding for example on a 32" or 48" pipeline, how many compressor machines and power rating. Location is not a matter of concept selection, and in case there are constraints those are considered. But environmental protection is not part of Safety anyways. Safety is a matter of design not of concept selection.
31	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	Which system properties are mainly considered in this process?	Economically (CAPEX, OPEX) and technically (annual throughput, expandability, flexibility) driven.	Performance goals (see 1), CAPEX and OPEX. However as written in 30, also Safety is considered to some extent.	Mainly economic factors. Safety is usually considered later in the development process.	Functional requirements combined with CAPEX/OPEX.	See 30. For example for selecting the location of the Tank Farm in Burgas the availability of fire fighting support in the surroundings as well as the proximity to a sport airport were considered. Also the location of the SPMs in the Burgas bay was selected considering the densitiy of exisitng vessel traffic. The location of the SPMs in the Alexandroupolis bay was selected considering the proximity to an exisiting military exercise area and seismic faults.	Not applicable in this project.	Functional requirements combined with CAPEX/OPEX.	Availability, CAPEX/OPEX.
32	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	Do you think it is possible to perform a sensible preliminary hazard analysis before a design is available?	Yes.	QRA cannot be performed without a relatively mature design. HAZOP is performed on PIDs. HAZID requires also some design performed.	Not discussed in interview.	No. See 30.	HAZID can be performed quite early (as it was the case in the Project).	No. For performing the QRA we needed a relatively developed design (safety-related philosophies were not available at the begining), so assumptions had to be made and later on as the design progressed the QRA had to be reviewed for possible change of results.	No. High-level system requirements (related to main parameters) must be confirmed and a certain design maturity is needed. For HAZID PFDs and preliminary layout were used. For HAZOP PIDs and Cause & Effect tables must be ready for approval.	No.
33	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	When should a preliminary hazard analysis be performed in a project?	At the very begining before starting design work.	Not discussed in interview.	Not discussed in interview.	As soon as possible.	Not discussed in interview.	As soon as possible.	See 32.	Not discussed in interview.
34	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	What do you understand as risk?	The probability that an adverse event might occur.							

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
35	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	Do you find it easy to estimate hazard likelihood?	No.	A design is needed for that.	No, however experienced practioners can come up with likelihoods which are then useful as basis for discussions.	In RAM (Reliability, Availability and Maintainability) Studies we can use OREDA (Offshore Reliability Data) and discussion on results are based on that data. There is not much "wiggle room". For QRA we also use OREDA (Offshore Reliability Data) and EGIG (European Gas Pipeline Incident data Group) for leak frequencies and estimation of probability of fire and explosion scenarios. QRAs process an incredible amount of data and assumptions, for example on leak frequencies, weather conditions, probabilities of fire and explosion scenarios, etc. Nowadays QRA S/W facilitates data management. There are many ways to adapt the results of a QRA by "fine-tuning" the many	No. For example we had to come up with an SPM frequency of leackage quite early in the Project, so that Environmental Consultant could perform QRA. That was a waste of time. This together with poor verification of QRA related assumptions led to stop the contract with Environmental Consultant. Moreover nobody understood how that figure was estimated and afterwards it was very difficult to justify its significance in the overall safety argument in front of the Bulgarian authorities.	In the Project we used OREDA data (Offshore Reliability Data) for estimating leak frequencies and equipment failures. But to me it is clear that those likelihood estimations can be manipulated to obtain an acceptable result (everybody knows).	Yes, leakage rates for example can be estimated according to operation experience. In this project however likelihoods were considered only in the SIL Assessment, QRA is not required by German Law.	In the QRA performed we used data from EGIG and other sources, however IOC-1 despite the fact that they have been operating the WAG system for 30 year, they did not have LOCs frequency data. IOC-1 learned a lot about QRA through our work and how frequencies can be used to develop a design rationale.
36	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	Do you think it makes sense to estimate likelihoods?	I have always doubts.	Yes, likelihoods provide a frame for priorisation of risks and decision making. How should we analyse risk then? what should we do with systems potentially subject to the so-called "Low Probability High Impact Events"? Not build those because such severe impacts are not acceptable (e.g. German policy on nuclear power)? The same applies to driving, should we stop driving? However I remember 20-30y ago the nuclear power industry safety standards were talking about accidents happening 1/1000y. I can think about 3 to 4 nuclear accidents which have happenned in these years.	Yes, they are useful for priorisation of mitigation efforts.For example IEC-60511 sets the frame for creating a rationale which can be audited afterwards aiding in justification in front of 3rd. parties. However some results of likelihood analysis are strange. For example a likelihood of BVS malfunction was analised in 1/167y (result from QRA in BTC Project). This figure is difficult to understand given that the system had been designed for a lifetime of 40y (what if that 1/167y is actually tomorrow? Macondo? Fukushima?). I am glad I don't work for the nuclear power industry.	For RAM Studies yes. See 35. For QRA not that much. See 35. Also how sure leaves us a QRA? When is enough enough? (Titanic, Fukushima). But on the other hand hazard likelihood is a good aid deciding where to make compromises because we cannot design for every accidental scenario. Another interesting example is that in the Crystal Gas Storage Project during the SIL Assessment the chairman pushed to try define a Compressor Unit incl. control system SIL 3, which has never been built in the world, the Vendor could not believe that. Fortunately operations practice were taken into consideration (complexity would have increased and it would have been difficult to handle). There is a lot of	It is very difficult if a design is not available.	If we have in the contract an Availability goal defined (e.g. 95%), then yes we shall use those Availability Studies for demonstrating that the system we have designed will fullfil that requirement. QRA frequency analysis is useful for deciding if a certain risk can be accepted or not. It helps discussing with the client which compromises might be done, because usually implementing all actions proposed for mitigating those fire and explosions has a huge impact in the project CAPEX and in the time schedule and we cannot even be sure if the system will be safe or not afterall. So it is useful to decide on trade-offs.	Yes, it is necessary for SIL Assessment and during operations for compliance with ABBergV and in order to comply with BSV a Gefährdungsbeurteilung (Hazard Analysis) has to be performed where likelihoods levels are assessed following the WEG Handlungsanweisungen (guideline for assigning likelihoods to events) (LP: this is not a probabilistic analysis though).	It all sounds very abstract. I have problems developing an opinion on what is acceptable and what not (F-N diagrams). Zero risk does not exist. What if I am "the" fatality in the 10,000 years?

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
37	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	Do you think it is possible to estimate likelihoods before a design is available?	No.	No. See 35.	No. For pipeline system projects it is normally assumed at the start of Basic Design that ESD systems are SIL 2 (PLCs in the market are usually SIL 2). For process plants projects we assume a SIL according to past experience of similar plants (i.e. what SIL "have" those in successfully operated similar plants?). Afterwards in Detail Design the same loops (now with more information) are evaluated. Sometimes a lower SIL is then obtained because other compotents in the loop (e.g. sensors avaialble in the market) are not SIL 2. Then if the SIL has to be higher "workarounds" such as increasing redundancy and maintenance are used, this is a well known practice accepted in the industry)	No.	No. See 36.	No.	No.	No.
38	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	What is your opinion about basing likelihood estimates on historical data?	In relative terms yes (events are more likely than others), but in absolute terms, I have doubts.	Not discussed in interview.	Not discussed in interview.	It is fine for RAM Studies, it is a good discussion basis. See 35.	Not discussed in interview.	Likelihood estimations can be based on data we have from past projects or operations experience.	It makes sense, for example we know leaks happen more often in compressors than in drums.	It is fine, there is data on which those can be based. See 35.
39	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	Do you find it easy to estimate hazard severity?	Yes, much easier than likelihoods.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	See 35. Fire and Explosion modelling can be very complex. With the aid of S/W it has become more manageable.	Not discussed in interview. Answer by Business Area 1 is considered representative.	We have used consequence analysis in the QRA.	Not discussed in interview.	We used an in-house Excel model for QRA.
40	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	Do you think it makes sense to estimate severities?	Yes.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Yes.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Yes.	Not discussed in interview.	Yes. It is a good way to assess adequacy of separation distances in station layouts and raise awareness about risk along the pipeline route.

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
41	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	Which elements of a hazard analysis process do you find most helpful towards overall preventing accidents (losses)?	QRA makes not much sense, to my opinion. More practical elements such as HAZOP or HAZID are more helpful. QRA has never had a further benefit than demonstrating the figures to an insurance contractor for example.	HAZID and HAZOP. QRA is also very important for evaluating individual and societal risk. It also helps verifying that the separation distances in the layout are adequate (heat radiation, overpressure). But for typical systems we engineer (e.g. pump stations), I don't think sophisticated safety studies are required, because the hazards are well known and the industry knows how to manage them. EC's project managers opnion is roughly divided into those who think the safety studies are a reasonable practice and those who don't.	HAZOP performed together with SIL Assessment is a useful exercise. It also aids in preparing component specifications and therefore obtaining comparables prices. QRA does not seem to have much impact on the design. For example the QRA prepared for BTC project was done a posteriori when the design had finished because the client wanted to have a justification that the design was fine.	HAZOP and HAZID. I like FMEA too, but it's very time consuming and therefore costly. The SIL Assessment is also a good confirmation of the design and HAZOP performed.	HAZOP.	HAZID, HAZOP together with SIL, QRA. Also Cause and Effect Charts. All have been very useful in the Project. The HAZOP performed together with the SIL Assessment was very good. The HAZOP sessions were too long. However the length/level of detail of these exercises is an issue. See 104. 2 to 3 weeks would have been a reasonable time frame. S/W PHA-Pro7 was very useful for facilitation of exercises. HAZOP is very useful, but it does not consider layout. QRA accounts for layouts. The Safety Layer Matrix Method as in IEC-61511-3 was used for SIL Assessment. SIL Target for loops was defined as SIL 2. If a loop was evaluated as SIL 4 or SIL 3, the design was considered not adequate	HAZOP. HAZID not that much. I don't think the FECA (Fire and Explosion Consequence Analysis) was needed, it shall be about not arriving to the point where a fire or explosion occurs. The Vibration Study performed was to demonstrate to the affected communities that some special fish types in a nearby river to Quarnstedt (the Quarnbach) would not be afftected by the operation of compressors. This is not a study normally performed. In my opinion it was not needed.	HAZOP together with SIL is very good (HAZOP identifies issues and SIL assesses them). This of course considering that the team works well together. Also Design Reviews as Approval Meetings with operations in this Project and/or dedicated reviews on safety, operability and maintainability are very useful. The QRA was very good for discussions and facilitated the rationale on mitigation measures such pipeline wall thickness, use of concrete plates por pipeline protection or pipeline lay depth, which are factors influencing the probability of a 3rd. party impact to the pipeline (the most famous example of that being a farmer performing earthworks).
42	Development	Conceptual Design	Level 1	Integrating safety into architecture selection and system trade studies	10.3.4	Which (traditional) hazard analysis technique do you consider most useful?	HAZOP and HAZID.							
43	Development	All	Level 1	Documenting environmental assumptions	10.3.5	What type of information related to system design and or hazard analysis do you understand as assumptions?	Data which the client is hesitating to confirm (e.g. Throughput data, oil and gas quality of new fields).	Not discussed in interview. Answer by Business Area 1 is considered representative.	Data/ philosophies not confirmed by client on which a design is based. For example regarding the security protection philosophy in the BTC project, it was assumed that the client was willing to implement standard solutions such as CCTV and fences. This was never discussed and it turned out to not be the type of solution expected by the client (whose policy was to employ local workers in the security monitoring). Ironically later on the concept was changed again to standard solutions.	Data not confirmed/discussed about the system design. Previous EC practice was to circulate PIDs through the different disciplines sequentially, so the first one commenting did not know what the last one would comment. This has now been changed, review meetings are performed. Also 3D walkthroughs are very useful exercises for verifying assumptions between different disciplines. This has now been introduced as standard.	Not discussed in interview. Answer by Business Area 1 is considered representative.	For example assumptions about the system design (safety-related design features). See 45.	Not discussed in interview.	For example the design of the compressor building had to be performed without knowing the type of compressor units which would be procured. But EC performed a good design for that due to previous experience. Another example of assumptions were the whole existing underground piping which had to be verified via survey.
44	Development	All	Level 1	Documenting environmental assumptions	10.3.5	Are assumptions usually recognized as such and documented in the system development process?	Assumptions are usually recognised as such, but sometimes, over the time, people forget that those were assumptions. Yes, in the Basis of Design.							

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
45	Development	All	Level 1	Documenting environmental assumptions	10.3.5	Are assumptions usually recognized as such and documented in the hazard analysis process?	Assumptions are usually recognised as such, but sometimes, over the time, people forget that those were assumptions. In particular this holds true for the hazard analysis because this exercise is usually performed at a later stage. Documentation of assumptions in the hazard analysis process is weak and very dependent on the team composition.	Not always, some yes.	Not always. During the design development, assumptions are sometimes forgotten and design solutions have to be changed eventually after significant rework. For example in the BTC Ceyhan terminal (Detail Design) the fire fighting monitoring system had been located during design in a building whose glass walls could not have withstood the heat radiation from a fire in a loading tanker. The assumption that those walls were fire resistant went from design to construction undocumented, and it was first identified during commissioning that this might have been an accepted risk. After much discussion the design was changed.	Not really. Sometimes hazard analysis are performed in a very superficial fashion (e.g. HAZOP Halfaya Project).	In this Project, Environmental Consultant had to make many assumptions in order to perform QRA because design was not developed enough at the point in time was contractually meant to perform QRA. EC verified assumptions and realised they were not sensible. Assumptions for QRA were documented in that case, but not in other hazard analysis. Other Project assumptions were documented in the Design Basis Memorandum. In the Oil Transportation Model assumptions were documented very detailed.	In this Project yes. Assumptions in hazard analysis were afterwards verified and the impact of changes assessed. However we did have a lot of problems with assumptions made in the pressure drop calculations (safety factors built in) and assumptions made in the piping design/ 3D model. The interface management did not work well there (Technip was responsible for the piping/ 3D modelling, EC was responsible for the pressure drop calculations and Tecon -an EC company- for the PIDs) so we had to perform walkthroughs to identify misalignments and perform recalculations. The interfaces were both of organisational and technical nature.	Not discussed in interview.	Not discussed in interview.
46	Development	All	Level 1	Documenting environmental assumptions	10.3.5	When should assumptions be identified in a project?	At the earliest possible stage	At the earliest possible stage and be verified and updated later.	At the earliest possible stage	At the earliest possible stage and be verified and updated later.	At the earliest possible stage	At the earliest possible stage and be verified and updated later.	Not discussed in interview.	At the earliest possible stage and be verified and updated later.
47	Development	All	Level 1	Documenting environmental assumptions	10.3.5	How critical do you understand are assumptions underlying the design and hazard analysis for safe system operation?	Fundamental.	Fundamental. Assumptions management is fine during Concept Selection and Basic Design due to the nature of the assumptions, they are high-level, of course if those change the impact can be enormous, but we manage to keep them known to the Project team. In the Detail Design phase it is a big issue. For example piping engineers and draftsmen assume all type of things when designing the piping in stations and they forget to record and communicate those to the Project team (e.g. gas storage Puchkirchen).	Fundamental. See 45.	Fundamental. Assumptions in a HAZOP changing over time might make operation procedures proposed not adequate anymore. Also Performace Standards for Safety Critical Elements and Safety related Devices (if prepared) define assumptions the systems shall fullfil. If after testing these cannot be confirmed (e.g. leak rates, opening/closing times, blowdown times, etc.), that shall be known by operations.	The IOC-5 Company never understood the assumptions underlying nor the "Oil Transportation Model" neither the "Oil Spill Model". The Tank Farms sizes were defined based on the results of the Oil Transportation Model, this is critical for CAPEX. The Oill Spill Contingency Plan for Operations was prepared based on the results of the Oil Spill Model.	Fundamental. See 45.	Not discussed in interview.	Not discussed in interview.
48	Development	Functional Design, Basic Design	Level 1	Generating system-level requirements	10.3.6	What do you understand as system-level requirement?	System-level requirement are requirements to the complete system as a whole to be engineered.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview.	See 1.
49	Development	Functional Design, Basic Design	Level 1	Generating system-level requirements	10.3.6	Do you recognise difference between system goals and system-level requirements? (NGL: Do you differentiate between system goals and system-level requirements?)	Yes, system-level requirements are measurable, goals can be more abstract (e.g. level of environmental compliance).							

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
50	Development	Functional Design, Basic Design	Level 1	Generating system-level requirements	10.3.6	Is formal documentation of (safety-related and not safety-related) system-level requirements usually practiced? If so, where in the project documentation?	Yes. In contracts and Basis of Design.	In the Basis Of Design.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Usually in Basis Of Design.	In this Project only Safety reports have been documented. Recommendations were not transposed to an specification.	In this Project safety-related requirements were developed and documented in the "Plant Safety Design Philosophy".	Not discussed in interview.	This was part of the Projekthandbuch (Project Manual). See 27.
51	Development	Functional Design, Basic Design	Level 1	Generating system-level requirements	10.3.6	Are (safety-related and not safety-related) system-level requirements traceable back to the system goals and/or hazard analysis from where they have been generated?	No. In exceptional cases yes.	Safety activities are documented, recommendations and actions are followed-up. Only if a DAL (Design Accidental Loads) Spec is prepared (IOC-9) then those requirements for buildings to withstand pressure and heat for example, or separation distances are traceable back.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not always, it depends on the project. Sometimes implementation of actions/recommendations is also not adequately performed. For example in the Eneco Project (LP: Underground Gas Storage faclity) EC was subcontracted the Detail Design by the ARGE (PPS, WSH, PLE). The HAZOP took only 2d and while the actions were administratively closed, the whole exercise was not taken seriously.	Not in this Project.	Yes. In this Project revisions of "Plant Safety Design Philosophy" and safety-related philosophies were progressively performed as hazard analysis and recommendations/actions were carried out.	Not discussed in interview.	Yes, for example laws provide requirements on noise restrictions which are then considered in the Projekthandbuch (Project Manual). See 50.
52	Development	Functional Design, Basic Design	Level 1	Generating system-level requirements	10.3.6	Is it later easy to see how these system-level requirements will be applied (i.e. for which decisions and/or design documents)?	No.	Through Project documentation references.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview.	Not in this Project.	Yes. Design development/revision was performed as hazard analysis and recommendations/actions were carried out.	Not discussed in interview.	See 50.
53	Development	Functional Design, Basic Design	Level 1	Identifying high-level design and safety constraints	7.3 10.3.7	Is formal documentation of (safety-related and not safety-related) system-level design constraints usually practiced? If so, where in the project documentation?	Yes, but not transparently in one single document Basis of Design, rather than indirectly.							
54	Development	Functional Design, Basic Design	Level 1	Identifying high-level design and safety constraints	7.3 10.3.7	Are system-level design constraints traceable back to the hazard analysis from where they have been generated?	No.	See 51.	Not discussed in interview. Answer by Business Area 1 is considered representative.	See 51.	Not in this Project.	Yes. See 51.	In this Project a FECA (Fire and Explosion Consequence Analysis) was performed by suggestion of EC (not required by client or law). This lead to requiring installation of light roofs in buildings and high strength concrete walls for occupied buildings (operation building and workshop).	These are the actions/recommendations in the HAZOP or QRA performed. Also in the minutes of meetings from related discussions.
55	Development	Functional Design, Basic Design	Level 1	Identifying high-level design and safety constraints	7.3 10.3.7	Is it later easy to see how these are applied (i.e. for which decisions and/or design documents)?	No.	See 52.	Not discussed in interview. Answer by Business Area 1 is considered representative.	See 51.	Not in this Project.	Yes. See 51.	See 54.	Yes, it can be seen in the Revision History of documents and drawings.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
56	Development	Functional Design, Basic Design	Level 1	Identifying high-level design and safety constraints	7.3	How are conflicts between generated system-level design constraints handled? (NGL: How are conflicts handled? Are they documented?)	Either system-level requirements are changed or the design has to be adapted accordingly. This usually has to be carefully discussed/agreed with the client. Conflicts are solved on a case by case basis and documented in contract changes or minutes of meetings.	Identified by Engineering Managers/ Project Managers and discussed in Project meetings together with client. Discussions are documented in Minutes Of Meetings.	Minimize investment seems to be the practiced policy.	On a case by case basis. There is no policy in EC. Lack of standard philosophies even leads itself to conflicts (internal and external). It is difficult to find consensus and after having solved issues claim management process is tedious. There is no "Technical Authority" (competence related) or "Chief Engineer" (technical authority in the company) roles in EC. According to my experience as "Process Technical Authority" at IOC-2 in the North Sea, project conflicts would be addressed to the "Technical Authorities" and in case those would not find consensus to the "Chief Engineer". But of course for most of the issues there was a policy and philosophies advising what to do.	In this Project, conflicts between design requirements and constraints have been handled in many meetings and documented in Minutes Of Meetings.	On a case by case basis. See 98 and 99.	Not discussed in interview.	See 98.
57	Development	Functional Design, Basic Design	Level 1	Identifying high-level design and safety constraints	10.3.7	Are system-level design constraints refined into more detailed design constraints? If so, are hazard analysis techniques used for that?	Not systematically.							
58	Development	Functional Design, Basic Design	Level 1	Identifying high-level design and safety constraints	10.3.7	Are system-level design philosophies developed into more detailed philosophies by domain expert engineers with the aid of industry/client standards? If so, do you think this is sufficient?	Usually design philosophies are issued only once at the begining of the project addressing system-level issues as well as component details. They are usually not revised into more detail for subsequent design stages.	Between Project phases yes (e.g. from Basic Design to Detail Design).	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not always. Also the level of detail of philosophies developed depends on clients and countries.	Not discussed in interview. Answer by Business Area 1 is considered representative.	In this Project the safety-related philosophies were further developed as hazard analysis were performed, not industry/ client standards aided. See 1 and 51.	Not discussed in interview.	Not in this Project. Design quite straightforward due to extensive experience.
59	Development	Basic Design	Level 2/ Level 3	System Design and Analysis (safety-driven design)	10.3.8	Where are the design principles usually documented?	Generally in the contract and especifically in the Basis of Design.							
60	Development	Basic Design	Level 2/ Level 3	System Design and Analysis (safety-driven design)	10.3.8	Is it clear where these design principles have been derived from (i.e. system-level requirements and design constraints)?	Yes, it is in subjectively 90% of the cases.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	See 58.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Yes, see 1 and 51.	From applicable norms and standards.	Yes. See 50 and 54.
61	Development	Basic Design	Level 2/ Level 3	System Design and Analysis (safety-driven design)	10.3.8	Are lower-level hazard analysis performed along with refinement of design?	Yes, HAZID and HAZOP.							

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
62	Development	Basic Design	Level 2/ Level 3	System Design and Analysis (safety-driven design)	10.3.8	How are the results of hazard analysis used in the design development?	Results do not always flow into the design. HAZOP recommendations related to changes in PIDs are usually implemented. Other hazard analysis exercises (e.g. QRA) are used ot prove that the design is "correct".	HAZOP recommendations are addressed (actions are followed-up and closed). HAZID and SIL recommendations are normally addressed too. QRA results are often not considered. The DAL Specification approach is sometimes implemented if the client requires (IOC-9).	Results of HAZOP and SIL Assessments are incorporated into design by revision of PIDs, C&E diagrams, and related operations philosophies. Results of QRA are somehow strange, see 36.	Design is revised according to recommendations/actions proposed (typically PIDs after HAZOP), also development of operation procedures.	HAZID results had a weak impact in the design. HAZOP results were implemented, QRA results had no impact at all.	Results of hazard analysis were mainly used to (i) revise the design and (ii) further develop safety-related philosophies. But also for highlighting safety-related issues in future operations (i.e. considering/ adressing issues in preparation of operation procedures).	Actions are closed out. PIDs are changed as indicated in HAZOP actions. FECA results (radiation and overpressure contours) were used to confirm safety distances/ change buildings design. SIL results were used to specify equipment/ items.	See 54.
63	Development	Basic Design	Level 2/ Level 3	System Design and Analysis (safety-driven design)	10.3.8	Which safety-related activities are defined as such in the system design process? When are those performed?	Often HAZID, HAZOP (most often, however if EC does not prepare PIDs, then it is not performed), SIL Assessment. Less often QRA.	HAZOP before approval of PIDs.	HAZOP before approval of PIDs sometimes performed along with SIL Assessment.	What is actually safety-related? Where does it start and where does it end? Typically HAZID, HAZOP and QRA. But also "Fire & Gas Detection Philosophy", "Fire Fighting Philosophy","Hazardous Area Clasisfication", "Fire Safety Plot Plans", "Venting Philosophy". But HP/LP Interface Register/Study, SRD Register/Study, LO/LC Register/Study, Performance Standards are not always seen as safety-related activities and most of times are not even performed/prepared (e.g. control of HP/LP Interfaces might require management of a lot of data implying having to implement a very strict change management process -e.g. in the Halfaya Project there are more than 800 HP/LP Interfaces). A typical HP/LP Register	In this Project, a general HSE Plan listing the HSE studies to be performed during the Project (HSE in Design) and also describing procedures for site visits was prepared. The so-called HSE studies include between others HAZID, HAZOP, QRA, ESIA, HSE Evaluation Criteria for EPC Tenders and LLI Supplier Tenders, HSE Inspection and Audit, HSE Traning Procedure, Noise Analysis and Mitigation Measures required, Hazardous Area Plot Plans, Fire Fighting Philosophy, Oil Emergency Response Plan.	See 106. In this Project HAZID, HAZOP with SIL, QRA. HAZID was performed relatively early in the Project. HAZOP with SIL were performed over 7w (4w system, 3w vendor packages) as PIDs have been developed. QRA was performed and revised for evaluating impact of changes on safety, also over a extended period of time. See 32.	In this Project HAZID, HAZOP, SIL, FECA (not defined, but performed, will not be part of permitting documentation, was prepared as result of concerns of affected communities about living close to a compressor station, only performed for CSs, not for MSs), Venting Study, Vibration Study (requested by affected communities) and a Pulsation Study (for piping).	For the Project the safety-related studies (HAZOP and QRA) were an option in the contract. Later on it was decided to carry out the option. EC provided the independent HAZOP leader for some of the HAZOPs, the rest were chaired by a 3rd. party. The QRA was rather a Project internal exercise, it never got submitted to the authorities. In Austria a lot of pipelines go through densily populated areas and in many communities pipelines are not even documented in the cadastral land registers and drawings. For the moment QRA is not a requirement to obtain permits. It seems there is a lack of awareness. However there are concerns about building new pipelines in the same route as exisiting ones (which bring already with
64	Development	Basic Design	Level 2/ Level 3	System Design and Analysis (safety-driven design)	10.3.8	Is there a set of safety-related activities which are always performed in all projects undergoing basic design by EC?	HAZOP only.	HAZOP is an established activity (in almost 100% of projects is performed). HAZID is performed in 70% of projects.	HAZOP only. HAZID and SIL Assessment sometimes.	HAZOP.	Not discussed in interview. Answer by Business Area 1 is considered representative.	HAZOP.	Not discussed in interview.	HAZOP.
65	Development	Basic Design	Level 2/ Level 3	System Design and Analysis (safety-driven design)	10.3.8	How are conflicts between design principles identified and handled?	By severe internal discussion, which happens very often.	See 56.	Not discussed in interview. Answer by Business Area 1 is considered representative.	On a case by case basis. See 56.	See 56. In this Project, conflicts between design requirements and constraints have been handled in many meetings and documented in Minutes Of Meetings.	On a case by case basis. See 98 and 99.	Not discussed in interview.	See 98.
66	Development	Basic Design	Level 2/ Level 3	System Design and Analysis (safety-driven design)	10.3.8	Are design decisions dealing with conflicts between design principles identified documented as such?	They are identified, but not always documented as such.	See 65. In Minutes Of Meetings.	Not discussed in interview. Answer by Business Area 1 is considered representative.	See 65. In minutes of meetings.	See 65. In Minutes Of Meetings.	See 65. In minutes of meetings.	Not discussed in interview.	Yes, in minutes of meetings. See 98.
67	Development	All	All	Documenting system limitations	10.3.9	What type of information related to system design and or hazard analysis do you understand as limitation?	Design limitations are issues specifically related to the project/system.							

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
68	Development	All	All	Documenting system limitations	10.3.9	Are limitations usually recognized as such and documented in the system development process?	Yes, very often limitations are not documented separately because they are considered known industry practice. For example some leak detection systems based on calculations and comparison of online data have a limitation regarding size of leaks (e.g. small leaks are not detectable).	Not discussed in interview. Answer by Business Area 1 is considered representative.	Yes. Limitations of (sub)systems are known to the industry. But documentation should be improved.	Not always. For example a good way to document assumptions/limitations of safety critical systems are Performance Standards. See 47.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Yes. Process limitations are documented in Basis Of Design.	Not discussed in interview.	Yes. Those are documented in Basis of Design, system/component specifications and are considered in contract awards to vendors.
69	Development	All	All	Documenting system limitations	10.3.9	Are limitations usually recognized as such and documented in the hazard analysis process?	Not systematically. Only sometimes.							
70	Development	All	All	Documenting system limitations	10.3.9	When should limitations be identified in a project?	If EC inherits a design developed by others, then related limitations should be identified as soon as possible after contract award and before further design work is performed. If EC develops design from concept selection, then limitations should be identified at certain hold points.							
71	Development	All	All	Documenting system limitations	10.3.9	How critical do you understand are limitations underlying the design and hazard analysis for safe system operation?	Limitations are usually better communicated during the design process.Therefore as opposed to criticality of Assumptions, it is a type of information usually known to designers and operators. Criticality for safe system operation is high.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Fundamental. As assumptions are. See 47.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Fundamental.	Not discussed in interview.	Fundamental. For example lube oil drums in compressor units are of 4,000 to 5,000 l. It is very difficult to detect leaks with those dimensions, however leak detection systems are specified SIL 3.
72	Development	All	All	Considering relevant operations experience in the development	12.1 13.2.6	Are lessons learned in operations (including accident and incident reports) considered in the development process?	Occasionally.	For example IOC-8 distributes so-called safety alerts and I am in their distribution lists. Those safety alerts report incidents. I usually forward those to the project managers I know are currently working in IOC-8 projects so that they take those lessons into consideration. Another example was an incident during commissioning of the BEP (Bunde-Etzel Pipeline) while pressurizing the line. I distributed the report to the people I thought might be interested. Of course lessons could be tranferrable to others, but well this is not analysed and distributed systematically.	When EC performed a design for a greenfield development and later on when the client wishes to perform a revamp of the facilities and EC is involved again. This happens often (e.g. MERO Pipeline where the greenfield project ca. 20y ago was designed for SIL 3 and SIL 4, as agreed between EC and the authorities, and it turned out to be very difficult to operate because of having to use very special PLCs and complex logic in order to fullfil such high target SILs. The revamp project recognised a reduction in complexity was necessary).	Lessons Learning seems to take place mainly through the enquiries of Regulators or when operators realize that the loss in reputation which is often a consequence of accidents/incidents might affect current and future business. When I worked for IOC-2 as "Process Technical Authority" I received reagular reporting on incidents happening in facilties in Germany. It is interesting to see how for example IOC-8 adopted the HSE assurance approach from the parent company in the US on top of compliance with German Law, however only got to understand the value once they had incidents in their facilities. It seems few organisations have specialised in HSE assurance in Germany (I can only think of TÜV)	In this Project we had a retired tanker captain consulting for the offshore design. He provided a lot of valuable information. For the onshore part we also had a senior operations specialist advising. We also visited the IOC-12 Oil Terminal Novorossiysk in the Black Sea and learned how they operated the terminal.	See 73. Also during commissioning a lot of learnign takes place. It is interesting because besides the process shutdowns identified/forecasted in safety-related philosophies and hazard analysis during commissioning new scenarios/ event chains also leading to process shutdowns have been identified. For example event 1, event 2 and event 3 had been studied separatedly and rated as not critical for plant status. But during commissioning new scenarios were created out of the interactions of conditions or influence of event 1, 2 and 3 between each other. These were not spurious trips. They have been studied -effects were not foreseen- and learning has been incorporated to operation	I was Operations Manager of a Gas Storage Site before, so in this Project operations experience and requirements has been considered, but I know it is not like this in other projects.	I am not aware about incident reports. However for example the draining system concept of filter/separators was changed in the frame of our Project through PID reviews (Approval Meetings) with operations and then they decided to change their philosophy for that.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
73	Development	All	All	Considering relevant operations experience in the development	12.1 13.2.6	How is industry operations experience considered in the development process?	EC tries to keep contact with operators, however not systematically and information communicated on experience is eventually located with individuals, rather than on a knowledge management database. If operators follow an Engineering Design Practice approach (e.g. IOC-2, IOC-6) then their particular experiences are considered by that means.	EC does not have an operations department, most of the learning we do about operations is during the commissioning phase which we support and through questions from clients during the guarantee periods we have to fullfil. It is however interesting that some operators (e.g. IOC-8) do not see the hazard of ignition of local vents (which is well-known) and they even tell us not to consider those in our Venting Studies. In those cases we even ask the client to sign a letter where they state they explicitely require us not to consider that hazard. Quite interestingly IOC-8 after a while changed their philosophy and now they do consider that hazard.	Mainly through client's Engineering Design Practices (e.g. IOC-2 ETPs, IOC-6 DEPs).	In general through the know-how of EC experts. But it is difficult to bridge the gap between designers and operators. Every designer has the problem about having insufficient experience/knowledge about operations. A typical operability/maintainability example are the so-called "sky-valves", these are valves which have been placed at high platforms/structures during design and the operators realize later that there is no access to them.	Not discussed in interview. Answer by Business Area 1 is considered representative.	In this Project mainly through EC's know-how. The client (IOC-13 and IOC-14) did not have experience in operating gas storage sites (IOC-13 have experience in nuclear power plants). See 77.	See 72.	In this Project operations got very involved because the WAG system is in operation since about 30 years, and the Project was an expansion of an exisiting system, so there was a lot of operations experience available.
74	Development	All	All	Considering relevant operations experience in the development	6.3.2	Are operations and maintenance engineers (EC's personnel and/or client's personnel) involved in development safety activities?	Operation and Maintenance personnel, in general, should be involved in the design, but as less as possible. Individuals or even some operators very often have their own particular ideas which do not reflect state of the art design practices, in contrary to written standards and regulations or design practices.	Operations representatives sometimes join HAZIDs and HAZOPs. Usually clients development and operations departments are not aligned (they have different interests and opinions about many issues), so it is difficult to obtain operations feedback because we mostly get to know people in the development departments. Operations people join the projects later during commissioning.	Many EC experienced engineers have been previously working for operators. Some first worked for EC, moved on to work for an operator and then came back. However there is no established process for either systematically involving those individuals or for involving clients' operations personnel in safety-related activities unless the client wishes to, which is sometimes the case.	Operators are not keen on sending Operations and Maintenance engineers to aid in the events hosted by designers because they seem to be always overloaded and the related costs do not seem to be justified. Every once in while they do get involved in HAZOPs, but it is/was rare even in my previous experience in IOC-2.	See 72.	See 75. The client (IOC-13 and IOC-14) did not have experience in operating gas storage sites (IOC-13 have experience in nuclear power plants). But they hired operations personnel during the development phase and got involved. Maintenance engineers have not been involved, maintenance programs were to be developed by the client (not in the scope of EC). The 3rd. Party certification body also got involved in the safety-related activities, their opinion was very useful to know when enough had been enough (in the analysis activities and in the design of systems).	See 72. Also IOC-16 operations was involved.	The system operations manager and the operations managers as well as field operators got involved in the safety activities performed (operations managers would consult specific issues with their operations and maintenance staff and provide information accordingly). For example the station layouts were discussed in the frame of Approval Meetings, especially the compressor building layouts. They also participated in the HAZOP and SIL and the results of QRA were discussed with them too. A HAZOP without operations makes no sense.

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
75	Development	All	All	Considering relevant operations experience in the development	6.3.2	Are field operators (client's or future operator's personnel) involved in development safety activities? If so, in which phase do they get involved? Do they get involved early enough?	No. In some cases their involvement might be useful, but it shall be remarked that the education levels sometimes are not sufficient for constructive discussions.	Not discussed in interview.	No.	Rarely. However in HAZOPs of operating systems they were involved (my previous experience in IOC-2). I was also assessor of technicians in IOC-2's CMAS process (Competence Management Assurance System). But the perception is that a fully automated system is safer than a system with operators. Human error is a complex topic, those are usually caused by systemic factors. However there are accidents which can only be explained by human error.	IOC-5 Company was created from scratch therefore no operators available.	In this Project we had a field operator (hired by the client) participating in approx. half of the HAZOP sessions. That was very useful because sometimes hazard analysis might get into very theoretic discussions and operators can easily provide valuable relevant information on specific issues (reality check).	Not in this Project.	See 74. Operations managers would represent the operations group in the meetings, field operators would not attend the meetings but issues were discussed with them (the operations manager would not just communicate his oipinion, but the opinion of the group).
76	Development	All	All	Considering relevant operations experience in the development	12.4	Do you think no accident (losses) of an operating system over a period of time is a valid legitimation of a system (design) as safe?	No. No losses might be "compensated" by very experienced operators or as a result of "chance".	No. No accident does not imply a safe design. For example many times there are LOCs (e.g. gas realeases) but nothing happens because the wind dilutes the gas cloud beyond the flamabillity limits or no ignition source is found, but that does not mean no incident can happen.	Not discussed in interview.	No. It cannot be stated that no accidents (losses) in an operating system over a period of time is an indicator that a design is safe. Successfully operating a system on such principle seems to me a matter of having had good luck. It is very difficult (if not impossible) to prevent accidents. 100% safety does not exist.	I think it's a 50%-50% relation. A design contributes so to say 50% to good operation with no losses, but 50% is about how the operator actually operates the system.	No.	Accidents can be prevented with good design and operating practices.	That is not a sufficient argument, operations experience has to be considered. For example in a HAZOP it is discussed about measures to prevent/mitigate freezing of air intakes, adequacy of/experience with design shall be discussed with operations. Maybe they have not had any incidents/ shut downs because of that, but operations says it is difficult to control that by inspection, so they would prefer to install an automated control for that. It depends.
77	Development	All	All	Considering relevant operations experience in the development	12.2	Do past clients (and/or operators) provide feedback to EC on their specific operation experience when safety activities were performed by EC as part of development work? If no, does EC obtain that information in an alternative form (norms, standards?)	It has happened in the past, but normally it is rare. We do get feedback sometimes informally through other sources.	This is usually by chance because we might be for example in a meeting with other participants from the same client which know also by chance about that plant we designed and they refer to it.	Yes, Informally through developed friendships with operators. Formally as explained in 72.	Not that I know.	Not relevant in this case. System has finally been awarded authority approvals last year. Not yet in operation.	EC's know-how on gas storage projects might have been fed by those (e.g. Epe, Puchkirchen, Eneco, etc.). This know-how is not systematically managed, but it is used in other projects.	Not discussed in interview.	In this Project operations got very involved because the WAG system is in operation since about 30 years, and the Project was an expansion of an exisiting system, so there was a lot of operations experience available. For example EC had performed HAZOP for the station Rainbach 2-3y before this Project in the frame of another project. The operations manager of that station had not changed in that time so he participated again and recalled issues.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
78	Development	All	All	Considering relevant operations experience in the development	12.2	Does operations feedback include (i) hazards which were overlooked or incorrectly assessed as unlikely or not serious; (ii) potential failures or design errors not included in the hazard analysis; (iii) identified hazards inappropriately accepted rather than being fixed; (iv) ineffective design controls?	If feedback is provided, sometimes through operator, but normally through other sources informally, then these issues are addressed.							
79	Development	All	All	Delivering safety requirements and constraints to operations	6.3.3 12.1	What type of information (safety information) is delivered by system engineering to operations for safe operation and maintenance?	Operation and Maintenance Manuals and training.	HAZOP recommendations including issues to be considered when writing operating procedures (e.g. make sure pig traps are depressurized before opening a pig trap door) are normally considered. HAZOP recommendations about changing PIDs are normally not. In some cases the client requires the complete HAZOP report as part of Final Documentation to be handed over to operations.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	In this Project, Operation and Maintenance concepts.	In this project operation manuals highlight sections which point safety-related issues with "warning signs" so that operators know the operation/procedure is safety-related and they shall be careful. HAZOP close-out reports indicate where in the operations manuals actions have been implemmented/ issues addressed. Operator's personnel has been trained using the operations manuals and awareness has been develop. See 86.	Not discussed in interview.	EC prepared a high-level operations and mainatenance concept and collected operations and maintenance manuals from vendors. In this Project IOC-1 developed themselves the operations and mainatenance manual which aligns the IOC-1 requirements (from the exisitng system) and the requirements of the vendors. This was the best way to do that in this Project. In other projects we do develop the operations and mainatenance manual, especially if clients (e.g. IOC-8) do not have experience with some parts of equipment, so we assist them on that.
80	Development	All	All	Delivering safety requirements and constraints to operations	12.1 13.2.6	Are operational assumptions, safety constraints, safety-related design features, operating assumptions, safety-related operational limitations, training and operating instructions, audits and performance assessment requirements, operational procedures and safety verification and analysis results passed to operations as part of the safety information "package"?	All this information is normally supposed to be included in Operation and Maintenance Manuals and training.							

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
81	Development	All	All	Delivering safety requirements and constraints to operations	13.2.6	Is traceability of safety information ensured between project phases and organizations involved? How does EC ensure or influence that?	EC tries through open communication with stakeholders, however very often it cannot be ensured.	Yes, through project documentation.	Not easy.	See 123.	It was not in this Project. See 4.	See 79. However operation manuals sections where HAZOP actions have been addressed do not point back to the HAZOP issues where they were identified/analysed. Hazard analysis reports are not part of final documentation.	Yes, it is easy in this Project because EC has worked in all engineering phases (Frame Agreement)	IOC-1 does not follow a facility lifecycle process (CVP Capital Value Process) as other operators do. Their are very experienced in so what they do is to award the complete engineering services to EC, so the main interfaces were between EC (designer), IOC-1 (client and operator) and the vendors. This contract model (of course supported by EC experience working with IOC-1) enabled fast track -a less sequential process- which otherwise would not have been feasible. HAZOP actions close-out regading operating procedures would be implemented by operations and EC would follow-up. IOC-1 was very experienced and their structures are very developed so that was the best way to manage that. See 79
82	Development	All	All	Delivering safety requirements and constraints to operations	12.4 13.2.6	Are client or future operators aware that the safety information created during development can be used generally for running an operations safety control structure and specifically for definition of indicators of system migration towards states of higher risk during operation?	Normally not.	Not always, some yes. See 79.	Not discussed in interview. Answer by Business Area 1 is considered representative.	It really depends on the client. For example Chinese clients are often not willing to pay for safety-related activities, therefore clearly not being aware about the importance of their results for operations.	Not discussed in interview. LP: In this Project most probably not, however the ESIA report proposes a lot of management (especially monitoring) measures which have to be fit into an operations safety control structure.	Yes, awareness is raised during operators' training.	Generally yes, although IOC-16 runs their so-called PIMS (Pipeline Integrity Management System) and that is already defined.	Yes, they were, that is one of the reasons why operations got so involved in this Project.
83	Development	All	All	Delivering safety requirements and constraints to operations	12.1 12.3	Are client or future operators aware that the safety information created during development can be used generally for running an operations safety control structure and specifically in safety change analysis to prevent system migration towards states of higher risk through changes during operation?	Normally not.	Not always, some yes. See 79.	Not discussed in interview. Answer by Business Area 1 is considered representative.	See 83.	Not discussed in interview. LP: In this Project most probably not.	Yes, awareness is raised during operators' training.	See 82.	See 82.
84	Development	All	All	Delivering safety requirements and constraints to operations	12.1	How is the safety information to be delivered to operations considered in training manuals and user manuals?	In related chapters.	See 79.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview.	See 79 and 81.	In Design Manual and Report which also includes the reports of all hazard analysis.	See 79 and 81.
85	Development	All	All	Delivering safety requirements and constraints to operations	12.1	Are safety-critical elements usually identified during development safety activities?	Not systematically.	Not discussed in interview.	Only if client requires for later priorisation of maintenance efforts.	With SIL Assessments. But for example we do not prepare SRD Registers or Performance Standards.	Not discussed in interview. LP: Probably not identified.	Yes, PIDs highlight safety-critical components such as HIPPS or pressure transmitters of ESD system.	Yes, in the SIL Assessment.	Yes, that was performed in the SIL Assessment.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
86	Development	All	All	Delivering safety requirements and constraints to operations	12.1	Is this information about safety-critical elements identified during development passed on to operations for establishing priority in maintenance plans?	Not systematically.	Not discussed in interview.	Only if client requires.	See 85.	Not discussed in interview.	Operations are responsible for the preparation of maintenance programes (not EC in this Project). Operations personnel has been trained and operation manuals clearly indicate safety-related issues, so that operations will be able to establish adequate priorities. See 85.	Yes, in the SIL Assessment Report and related specs.	Requirements for maintenance are defined by the results of the SIL Assessment.
87	Management	All	Level 0	Providing leadership for safety matters	13.1	Do you think investing in safety makes sense?	Yes.							
88	Management	All	Level 0	Providing leadership for safety matters	13.1	What are the returns of investing in safety?	Prevention of losses and economical advantages.							
89	Management	All	Level 0	Providing leadership for safety matters	13.1	Do you think EC type of industry is more/less hazardous than others?	More hazardous than others.							
90	Management	All	Level 0	Providing leadership for safety matters	13.1	Do you think accidents are the price of productivity and anyways cannot be eliminated?	No.							
91	Management	All	Level 0	Providing leadership for safety matters	13.1	Do you think accidents (losses) are random events?	No.							
92	Management	All	Level 0	Providing leadership for safety matters	13.1	Do you think accidents (losses) can be prevented?	Yes.							
93	Management	All	Level 0	Providing leadership for safety matters	13.1	Do you think safer systems cost more than others? (NGL: Are safer systems more expensive to produce? To operate? Overall?, What penalties or costs are required to get safer systems?)	The initial investment is higher, but it pays off over the lifetime.							
94	Management	All	Level 0	Providing leadership for safety matters	13.1	Do you think that designing safer systems requires unacceptable compromises with other goals?	Sometimes yes.							
95	Management	All	Level 0	Providing leadership for safety matters	13.2.1	How often does management deal with safety issues?	Weekly.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	In my case 30%-40% in the last quarter.	Not discussed in interview. Answer by Business Area 1 is considered representative.	I dealt with safety issues on a daily basis. I am project manager and lead process engineer so many issues come back to me in any case.	Not discussed in interview.	I was very often involved in safety discussions. For example in the frame of Approval Meetings there were always safety-related issues to be discussed.
96	Management	All	Level 0	Providing leadership for safety matters	13.2.1	Does management participate in safety efforts?	Project Managers very often. Line Managers not.	Very dependent on the particular Project Manager's approach.	I have been not involved in a Risk Assessment such as HAZID or HAZOP for years. In SIL Assessments every once in a while.	I have been very involved in safety-realted activities for the Halfaya Project: (i) in the HAZOP as team member (note: only 2d HAZOP), I have written myself the Health Check Report and lead/written the LP/HP Interface Study.	The Engineering Manager and myself (Project Manager) were involved at the begining of the Project (we defined together with IOC-5 Company the Risk Criteria) and during the development as necessary, however not systematically. A so-called Technical Safety Manager (to differentiate from Occupational Health and Safety) should always be part of the Project Organisation in the Engineering group to manage this consistently.	I participated in all safety efforts including following up actions.	Not discussed in interview.	As a project manager besides the discussions in Approval Meetings (see 95), I participated in the HAZOP+SIL and in the discussions of QRA results. I also checked related reports.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
97	Management	All	Level 0	Implementing a safety policy	13.2.2	Does EC implement a safety policy?	Yes.	Yes, but it is very high-level.	Yes. However it seems more an Occupational Safety policy rather than a policy on how to design safety in systems.	Not for projects.	The Project HSE Plan included it.	Not for projects. Safety Minimum Requirements or Recommended Practice (RP) was not available in EC. For example a RP should include (i) minimum safety distances recommendations and (ii) escape route design recommendations -API escape routes RP exist, but in EU there is not such-. Since the client did not have such standards (i) every safety-related philosophy had to be developed form scratch, (ii) there has been a lot of discussions on safety-related matters and (iii) it has been difficult to issue change orders because there is no basis to argue upon, so client simply does not accept certain proposals. A proper standard which is discussed/ used from the begining of the Project	Not discussed in interview.	When the Project started at the end of 2005 IOC-1 did not have a policy for design (safety-related philosophies). Later on in 2008 they developed an HSEQ policy which included risk assessments to be performed, that was considered in the new projects. But that was nothing like a design standard. IOC-9 implements those (e.g. specifies minimum separation distances between process areas and buildings). EC does not have a documented policy as far as I am concerned. What we do is preparing a draft design according to experience and old projects and then we evaluate it with HAZID, HAZOPs, etc. A recommended practice might be helpful, but that might be difficult because
98	Management	All	Level 0	Implementing a safety policy	13.2.2	Does EC's safety policy clearly define the priority between conflicting goals (i.e. between safety and other goals) to be used in decision making?	Yes. However reality sometimes deviates.	No. It is very high-level and it is not easy to use as guideline for project work.	No. It is very high-level and it is not easy to use as guideline for project work.	No. See 56.	Not discussed in interview.	No. See 97. We have had very intense discussions not only with the client, but internally. IOC-13 is used to the Nuclear Power Industry standards (not experienced in gas storage facilties, very high risk perception), also the new Technical Safety Manager recruited by EC for the Project had past experience working for IOC-15 and LNG plants, so together while developing the safety-related philosophies a very high Safety profile in the design was being developed, which on the other hand conflicted with the common practice from EC in other projects and overall pushed the costs up. Also this developed in establishing a very high Safety profile for the Etzel site in general because the 3rd party certification body was keen on keeping the same	Not discussed in interview.	No. Conflicts are solved on a case by case basis. A typical example is recommending to install collecting traps (secondary containment without high walls) for coolers. We consider this only solves one part of the problem (i.e. what if the leak is spilled over the trap? -there are no walls- in that case building a trap with higher walls would impair ventilation creating another hazard). For bateries this is an adequate solution.

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
99	Management	All	Level 0	Implementing a safety policy		Does the safety policy provide the scope for discretion, initiative and judgement in deciding what should be done in specific situations?	No.	No. It is not regulated how to decide when safety conflicts with other Project goals such as minimizing CAPEX. This is done on a case by case basis. Project managers are afraid to increase project costs by incorporating safety features and often our clients too. For example in the Gas Storage Crystal EC Technical Safety Manager proposed to install collecting trays under a pipe bridge with condensate. German norms do not require those trays/pits if the piping does not have flanges, which was the case. However the Technical Safety Manager insisted in incorporating those to collect the condensate in the event of leckages/ ruptures. This would have been a significantly expensive measure which project	No.	See 98.	Not discussed in interview.	No. Every issue had to be discussed on a case by cases basis. See 98. We would have saved money and time if this had been defined.	Not discussed in interview.	No, see 97 and 98.
100	Management	All	Level 0	Implementing a safety policy	13.2.2	What are the elements of EC's safety policy? Does it contain (i) goals of the safety program; (ii) criteria for assessing short- and long-term success of that program; (iii) values used in tradeoff decisions; (iv) clear statement of responsibilities, authority, accountability and scope?	(i) yes, other elements no.							
101	Management	All	Level 0	Implementing a safety policy	13.2.2	Is EC's safety policy explicit and clear so that it can be operationalized?	No.							
102	Management	All	Level 0	Implementing a safety policy	13.2.2	Do you believe that EC's safety policy reflects true commitment by management?	Yes.							
103	Management	All	Level 0	Implementing a safety policy	13.2.2	Do you believe you will be supported by management if you choose safety over the demands of production?	Yes.							

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
104	Management	All	Level 0	Implementing a safety policy	13.2.2	Do project schedules allow for delays due to safety concerns?	In most cases not. It depends on how "progressive" the client is.	No. Therefore it would be important to evaluate system safety early enough in the Projects, so that changes can still be performed if necessary. But this is again something primarily influenced by the Project Managers.	Not discussed in interview. Answer by Business Area 1 is considered representative.	No. For example HAZOPs if they are included in time schedules, normally they are not assigned sufficient time (e.g. Halfaya Project HAZOP 2d). Too much PIDs changes after a design has been frozen lead to schedule delays. That is an indicator that the PID reviews, the HAZOPs and the HAZOP actions close-outs have not be performed adequately.	In this Project no.	The Project schedule did not even account for the time required for hazard analysis. For example in this Project we had a 7w series of HAZOPs together with SIL (4w system, 3w vendor packages), which was excessive because everything was a discussion point (again no standards/philosophies) and because the HAZOP Chairman which was payed by the client (not truly independent) clearly wanted to distinguish in the exercise. These are also important factors.	See 5.	A good time schedule should allow for design corrections after a hazard analysis is performed. But on the other hand a hazard analysis recommending a lot of changes in design is a sign of bad quality of the design performed (= too much re-design). Also if changes imply significant project delays, the time schedule most probably was not adequate. It is also important to assess the impact of changes in design triggered by safety concerns considering operations practice before measures get approved (e.g. proposing to incorporate a safety valve in Filter/Separators might be generated in an specific HAZOP node, but then implementing that in other parts of the system -philosophy- can overall be costly and time consuming
105	Management	All	Level 0	Implementing a safety policy	13.2.2	Are the employees aware about EC's safety policy? How is this achieved?	Too less.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Yes. But as stated in 98 they cannot use it for their daily work.	There is no such policy for projects. See 97 and 98. Safety Alerts distributed to personnel with for example abstracts of safety-related articles, incident reports, etc. would be useful to improve that. A safety column in the EC News (internal newsletter) would be a good idea too.	Not discussed in interview. LP: The Project HSE Plan included a so-called HSE Awareness Training for all parties joining the Project. Records have not been found.	See 97.	Not discussed in interview.	There is no such policy for projects. See 97 and 98.
106	Management	All	Level 0	Implementing a safety management plan	13.2.7	Are project specific development safety management plans usually prepared as part of project set-up?	Only if client explicitely requires.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Only if client requires it and usually those are general HSE plans (HSE in Design).	See 93. This HSE Plan complies with industry practice but does not clearly regulate how to integrate safety in system engineering. This is a common pitfall in many projects, those plans do not get operationalized. Also general HSE Plans as understood by many operators include System Design and Occupational Health and Safety together.	In this Project a so-called "Plant Safety Design Philosophy" was prepared pointing at all the other activities and documents to be prepared (e.g. Hazardous Area Classification and Drawings, Fire Detection Philosophy, Fire Detection Philosophy, Venting Philosophy", etc.). We needed to organise the whole Safety effort.	Not in EC's scope in this Project.	In the projects where I have been project manager, the time schedule lists all safety-related activities with their links to predecessors (inputs) and successors (outputs), so it is a powerful planing tool. Since such a request was never part of IOC-1s requirements at that time, we did not prepare a special plan for it, but those studies were included in the time schedule.
107	Management	All	Level 0	Implementing a safety management plan	6.3.1	Does management think that project specific development safety management plans are necessary?	Not in all cases.							

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
108	Management	All	Level 0	Implementing a safety management plan	12.7 (guideline adapted to development phase: minimum reqs.)	Do project specific development safety management plans address the following elements: (i) Scope and objectives, applicable standards, documentation and reports; (ii) safety organization (roles and responsibilities, coordination, system safety interfaces with other groups); (iii) procedures (hazard and risk analysis, safety-driven design, management of change, training, decision-making and conflict resolution); (iv) schedule of safety activities (milestones, checkpoints, timing of activities, reviews and required participants); (v) safety information system (hazard and risk analysis, hazard logs, hazard tracking and reporting systems and applicable lessons learned)	Only if client explicitely requires.							
109	Management	All	Level 0	Implementing a safety control structure	13.2.6	Is there a group in EC responsible for safety in the projects? If so, where is it usually placed in the project organization? Where is it placed in EC organization?	Not visibly. Not in the organization.	No. This is being discussed at the management level so that a separate safety group will be created.	Not discussed in interview. Answer by Business Area 1 is considered representative.	The safety group is not established in the organization and it is not visible.	See 96. A so-called Technical Safety Manager (to differentiate from Occupational Health and Safety) should always be part of the Project Organisation in the Engineering group to ensure Safety is considered.	At the time the Project started (Jan 2009), there was no such a group, so we had to recruit an experienced Technical Safety Manager and subcontracted the QRA to Weyer Group. Somehow knowledge was there but disseminated/ not centralised and no dedicated personnel was available for that. I know now there is dedicated personnel to Safety in the organisation.	We have used engineering team members for performing those. Also Certification Party (LP: independent 3rd. Party certification) has participated. I am not aware about a Safety Group.	The ultimate responsible authority in the project is the project manager. I don't know about any safety group as such, but I know who performs such activities in EC.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
110	Management	All	Level 0	Implementing a safety control structure	13.2.6	Do you think safety efforts have an impact on the system design EC produces?	Generally yes.	Yes.	Generally yes. However as for the safety efforts of GB-I (e.g. Specification of fire and gas detection systems, leak detection systems, SIL Assessments, etc.) they usually come rather late in the design so that the efforts focus a lot on adding safety features to the design other disciplines (process, mechanical) have performed before in an intent of mitigating hazards not identified or addressed in the design development before. For example one of the factors for preventing LOC (Loss Of Containment) in a pipeline is the pipeline wall thickness. This hazard can be effectively mitigated mechanically, i.e. increasing wall thickness, however this is not feasible because pipeline wall thickness is a major cost driver in a project (amount	The safety efforts find their way into design, however not efficiently and often too late. And surely we do not dedicate enough efforts to safety.	In this Project, the aspects addressed by the ESIA, as explained in 31, did have a significant impact (decisions on route and location were taken considering Safety and Environmental concerns). HAZID results had a weak impact in the design. HAZOP results were implemented, QRA results had no impact at all. Overall the whole exercise was used to obtain permits from authorities and justify compliance with European Seveso II Directive.	In this Project absolutely. All actions had been followed-up and the safety-related philosophies and design features implemented can be traced back to the hazard analysis performed.	See 62.	Yes.
111	Management	All	Level 0	Implementing a safety control structure	13.2.6	Do you think safety efforts are part of mainstream system engineering in the projects?	No.	Partly. Some Project Managers in EC and other people do not see those as necessary.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Currently not, but will be.	In this Project, Safety and Environmental considerations were practically part of maintream engineering for route and locations selection. In Basic Design and FEED no. Generally no. They should be integrated in the engineering process.	No, they are not. Special know-how is needed for that and not every engineering company has developed those.	Mechanical and instrumentation engineers do design safety-related systems such as HIPPS (High Integrity Pressure Protection Systems).	In the projects where I have been project manager, yes. But I cannot generalize for EC.
112	Management	All	Level 0	Implementing a safety control structure	13.2.6	Are safety-related design decisions taken independently of project managers (who are usually governed by cost, schedule and mission accomplishement goals)?	No.							
113	Management	All	Level 0	Implementing a safety control structure	13.2.6	Do you think the safety group enjoys the prestige necessary to have influence on decision making that safety requires?	No, but growing.	Who is actually the safety group? You guys? See 109.	Not discussed in interview. Answer by Business Area 1 is considered representative.	No, safety groups usually do not have enough practical influence in decisions (not even in IOC-2, according to my experience).	No. Safety efforts are a bit like QA/QC or Occupational Health and Safety satellites.	I know now there is dedicated personnel to Safety in the projects.	I am not aware about the safety group.	Project manager is the authority for decision making. The safety group is responsible for performing analysis and supporting the projects. This is how it worked in this Project.
114	Management	All	Level 0	Implementing a safety control structure	13.2.6	Are there safety working groups (not the groups responsible for safety mentioned above) in EC?	Virtual Competence Team on Technical Safety.							
115	Management	All	Level 0	Implementing a safety control structure	13.2.6	Does EC implement corporate development safety standards? What are the minimum requirements, if defined?	No, but there is a program to develop it for Oil & Gas Business Field.	Not discussed in interview. Answer by Business Area 1 is considered representative.	Not discussed in interview. Answer by Business Area 1 is considered representative.	No, this is a problem. Minimum requirements shall be developed.	If any available, they were not used in the Project.	No. See 97. EC needs to develop those.	Not discussed in interview.	No.

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
116	Management	All	Level 0	Implementing a safety control structure	13.2.6	Does EC implement management of change evaluating impact of changes on safety?	No.	I am a fan of the Management of Change process. We have a Management of Change process, however it is not implemented in a systematic way and many times inconsistencies and related problems are identified later during the construction phase or even during operations. It is a beneficial process not only for Safety but in general for any engineering aspect.	No.	No, this is a problem. Change Management shall be implemented, not only for safety-related issues, but for any engineering activity.	In this Project, Environmental Consultant had to make many assumptions in order to perform QRA because design was not developed enough at the point in time Environmental Consultant was contractually meant to perform QRA. EC verified assumptions and realised they were not sensible. When it was requested to revise the QRA considering newest information which had superseeded the assumptions, Environmental Consultant was not willing to revise the QRA (most probably because it is a lot of work which they were afraid not to get payed for). So changes in safety could not be evaluated.	In the Project we did evaluate impact of any changes mainly using the QRA software. But Change Management is not only important for Safety matters, it is fundamental for any changes in the project. Project teams need to develop "claim awareness", so that changes and their impacts also to EC's workload can be transferred to clients (currently there is little awareness about the importance of communicating changes within project teams).	Changes in main parameters (e.g. operation points) triggered a major redesign therefore change management had to be performed. The results of Hazard Analysis were somehow reused from one Compressor Station and/or Metering Station. Differences between the stations were considered were applicable.	Not in a systematic way. I am actually not a friend of procedures, but I do see the importance of formalising Management of Change. For example in one project we had changes during construction, however we did not sufficiently analyse the extent of the impacts on other parts of the system, which we should have done.
117	Management	All	Level 0	Implementing a safety control structure	13.2.6	Do you think EC provides sufficient resources for safety-related activities?	No, but growing.	No.	Always short in resources. For example, currently in the IOC-11 Full Field Development Project Portfolio (E858), we do not have enough HAZOP leaders and this has been a major issue.	See 118.	Not for this Project. And generally no. See 109.	See 109. See 104.	Not discussed in interview.	Yes, I have never had a problem to obtain resources for safety-related activities, maybe because I know the people who I have to talk to and eventually, if not on a timely manner, I have been supported. But in general (not only for safety-related matters) that might be an issue.
118	Management	All	Level 0	Implementing a safety control structure	13.2.6	Do you think employees performing safety-critical activities have the appropriate skills, knowledge and resources for that?	No, but growing.	Only one senior member has a lot of operations experience. The rest should gain experience regarding operations (e.g. be sent to participate in commissioning activities)	Not discussed in interview. Answer by Business Area 1 is considered representative.	For Upstream faiclities it is increasingly important to have certified personnel, even Russian clients (e.g. Lukoil) are asking for certified specialists (e.g. TÜV Functional Safety Engineer). This is actually very important for Detail Design or in general for Project Execution related contracts because once a project reaches the Execution phase it means sanctioning has been awarded and whatever is built will be operated (there is more certainty about the realisation therefore teams get more concerned about what and how things are performed). It is interesting to note that a lot of incidents occur in flare, venting and drain lines whose design is normally a task assigned to junior engineers.	In this Project, EC had to subcontract ERM for that part of scope and unfortunately the results were not satisfactory, having to redo the QRA ourselves and not being able to deliver an integrated concept for ensuring safety. In general it is not clear where the so-called Technical Safety group is in the organisation, i.e. what are actually the resources available for safety-related activities?	See 109.	Not discussed in interview.	Yes.
119	Management	All	Level 0	Implementing a safety control structure	13.2.6	Do you think employees performing safety-related decisions are fully informed and skilled?	No, but growing.							

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Q No.	Element Sys Eng	Project Phase	Intent Spec	Element of Using STAMP	Chapter	Question	Business Area 1	Business Area 2	Business Area 3	Business Area 4	Project 1	Project 2	Project 3	Project 4
120	Management	All	Level 0	Implementing a safety control structure	13.2.6	Do you think EC performs high-quality and comprehensive hazard analysis?	It depends on the stakeholders which participate in the exercises.							
121	Management	All	Level 0	Implementing a safety control structure	13.2.6	Do you think results of hazard analysis are usually considered when safety-related decisions are to be made?	Not systematically.	Yes.	Results of QRA are not really considered for decisions (see 41). However other results provided by HAZOP or SIL do usually find their place in safety-related decisions.	Generally yes, but there are conflicts, see 56.	In this Project yes (in practical terms), as mentioned regarding route and locations. However not formally, the different studies were never considered Hazard Analysis. HAZID results had a weak impact in the design. HAZOP results were implemented, QRA results were not considered at all.	In this Project absolutely.	See 5. See 62.	Yes, in this Project they were. HAZOP actions were followed up and considered as well as the results from QRA.
122	Management	All	Level 0	Implementing a safety information system	13.2.7	Does management think that a project safety information system is necessary?	Most do not.							
123	Management	All	Level 0	Implementing a safety information system	13.2.7	Do projects implement a safety information system? (NGL: What kind of safety information exist? How is safety information documented and communicated in projects? Among projects?)	Only if client explicitely requires.	Yes. Every Safety activitiy or study is documented and clients can use those results if they wish. For example HAZOP and HAZID reports and their action lists are part of the Project documentation.	Not discussed in interview. Answer by Business Area 1 is considered representative.	That is again very client dependent and if so not to the extent of my experience at IOC-2 in the North Sea, where for example a centralised action tracking system for all platforms/projects/organisations in the North Sea was established. Of course we might not need that level of control for our projects, but something similar would help.	Not in this Project. Recommendations lists and Safety Reports in general were managed like any other document in the Project Sharepoint. Communication of safety information between disciplines/ stakeholders was highly dependent on the time managers (Engineering Manager or even Project Manager) had for that. No established process.	See 106. All safety-related philosophies were have been developed as indicated in the hihg-level document "Plant Safety Design Philosophy". Every hazard analysis and their revisions have been documented and all actions closed-out. Any safety-related decisions in discussions has been documented in minutes of meetings.	Not in this Project.	There was not a especial system for that. In this Project through reports and registers and operation and maintenance manuals from vendors. This was managed in a document management system.
124	Management	All	Level 0	Implementing a safety information system	13.2.7	What are the elements of a project safety information system? Does it contain (i) development safety management plan; (ii) status of safety-related activities; (iii) safety constraints and assumptions underlying the design, including operational limitations; (iv) results of hazard analysis (hazard logs) and assessments; (v) tracking and status information on all known hazards; (vi) lessons learned and historical information?	Usually according to client requirements. (iii) no, (vi) usually no. Other yes.							

Legend:
blue: question answered only by Business Area 1
grey: answer by Business Area 1 representative
pink: question not discussed in interview

Appendix 2 Project Example

Table of Contents

List of Tables and Diagrams

Glossary of Terms

Engineering a Safer World

Leveson, N. G., 2011. Engineering a Safer World. Systems Thinking Applied to Safety. MIT Press, Engineering Systems Series. ISBN 978-0-262-01662-9, Jan 2012.

Safety

Absence of fatalities and injuries during system operation.

Limited definition for the purpose of this thesis derived from Leveson's definition of safety as freedom from accidents (or loss).

Safety-related

Something which might influence safety, i.e. project activity which might influence the absence (or presence) of fatalities and injuries during system operation.

VISION

Heriot-Watt University's Virtual Learning Environment. It is a web-based integrated teaching and learning environment.

Nomenclature

A	Accident
BVS	Block Valve Station
CIS	Commonwealth of Independent States
COESD	Controlled Operation Emergency Shut Down
DEP	Design Engineering Practice
DEUDAN	DEUDAN Gas Pipeline which connects the German and Danish gas networks
EC	ENGINEERING CONTRACTOR
e.g.	An abbreviation of Latin “exempli gratia”
	e.g. is often used to introduce an example. It is sometimes pronounced as “for example”
EGIG	European Gas Pipeline Incident data Group
EPC	Engineering Procurement Construction
ESD	Emergency Shut Down
ESIA	Environmental and Social Impact Assessment
ETP	Engineering Technical Practices
FEED	Front End Engineering Design
FFS	Fire Fighting System
F&G	Fire and Gas Detection System
FPS	Flow Path Supervision
G	Goal
GB	Geschäftsbereich (=Business Unit)
GB-A	Business Unit-Acquisition
GB-B	Business Unit-Business Services
GB-C	Business Unit-Gas Compressor Stations
GB-E	Business Unit- Electrical Power Systems
GB-I	Business Unit- Instrumentation, Automation and Telecom
GB-L	Business Unit-Tank Farms and Terminals
GB-M	Business Unit-Pipeline Systems
GB-P	Business Unit-Project Management
GB-S	Business Unit-Process Facilities
GB-U	Business Unit-Upstream
HSE	Health, Safety and Security, and Environment protection
HAZID	Hazard Identification study
HAZOP	Hazard and Operability study
ICSS	Integrated Control and Safety System

IDS	Intrusion Detection System
i.e.	An abbreviation of Latin “id est” i.e. is often used to explain or clarify a statement. It is sometimes pronounced as “that is”
IEC	International Electrotechnical Commission
IMS	Integrated Management System
IOS	Integrated Open Season
IT	Information Technology
LCC	Local Control Centre
LDS	Leak Detection System
LOC	Loss Of Containment
MCC	Main Control Centre
MTA	Million Tons per Annum
MTBF	Mean Time Between Failures
MTTR	Mean Time To Repair
Nm^3/h	Normal Cubic Meters per Hour
OREDA	Offshore Reliability Data
PCS	Pressure Control System
PID	Piping and Instrumentation Diagram
PMC	Project Management Consultancy
QRA	Quantitative Risk Assessment
SCADA	Supervisory Control and Data Acquisition
SCS	Station Control System
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
STAMP	Systems-Theoretic Accident Model and Processes
STPA	Systems-Theoretic Process Analysis
UCA	Unsafe Control Action
WAG	West-Austria Gas Pipeline

References

[1] Leveson, N. G., 2011. Engineering a Safer World. Systems Thinking Applied to Safety. MIT Press, Engineering Systems Series. ISBN 978-0-262-01662-9, Jan 2012.

[2] -deleted

[3] IEC 61511-3. Functional Safety – Safety Instrumented Systems for the Process Industry Sector. Part 3: Guidance for the determination of the required Safety Integrity Levels. Ed. 1.0 2003-03.

[4] -deleted

[5] Trans Balkan Pipeline, 2012. Website. Available from http://www.tbpipeline.com/ [Accessed 15 March 2012]

[6] DEEP, KBB, EKB, E.ON, IVG, JadweBay, OMV, Statoil, VNG, 2011. Cavern Storage Etzel. Securing Supplies of Natural Gas and Oil. Available from http://www.jade-bay.de/ [Accessed 15 March 2012]

[7] Gasunie, 2010. Gasunie to tackle Security of Supply Bottlenecks. Available from http://www.gasunie.nl/ [Accessed 15 March 2012]

[8] Gasunie, 2011. Projektinfo Quarnstedt. Available from http://www.erdgas-fuer-morgen.de/ [Accessed 15 March 2012]

[9] Gasunie, 2011. Einwohnerversammlung Quarnstedt Neubau Verdichterstation. Available from http://www.erdgas-fuer-morgen.de/ [Accessed 15 March 2012]

[10] -deleted

[11] -deleted

[12] -deleted

[13] -deleted

[14] -deleted

[15] ISO, 2000. ISO 17776 "Petroleum and natural gas industries —Offshore production installations— Guidelines on tools and techniques for hazard identification and risk assessment". ISO 17776:2000(E)

[16] -deleted

[17] -deleted

[18] -deleted

[19] -deleted

[20] -deleted

[21] Fleming, C, Leveson, N.G., Spencer, M., (Massachusetts Institute of Technology), Wilkinson, C. (Honeywell Aerospace Advanced Technology, Columbia, Maryland). Safety Assurance in NextGen. NASA. NASA/CR-2012-217553, March 2012.

[22] Thomas, J., 2012. Extending and Automating STPA for Requirements Generation and Analysis. Presentation in 1st STAMP/STPA Workshop 18.04.2012.

[23] -deleted

1 Introduction

This appendix describes how the new techniques have been applied to a real project currently being processed by EC. The STAMP Elements addressed in this example include only the Engineering Development elements and the interface elements to Operations. Management elements related to EC have not been addressed.

1.1 Definition of Safety

Safety is defined in Engineering a Safer World as freedom from accidents (or loss events). This is a holistic definition which implies that any type of loss event impacts on safety. The Oil & Gas industry uses a more limited definition of safety the common understanding of which could be articulated as the absence of fatalities and injuries. Some operators do extend the definition of safety to HSE (Health, Safety and Security, and Environment protection). Some also like to consider impacts on Assets, Productivity and Reputation in the scope of HSE.

The analysis below is developed based on the limited definition of safety as absence of fatalities and injuries during system operation. Safety-related is defined herein as something which might influence safety, i.e. project activity which might influence the absence (or presence) of fatalities and injuries during system operation.

However it is observed that the potential of the new techniques goes beyond this limited definition. This might be subject of further study (i.e. engineering to avoid any identified project or system losses).

1.2 Project description

The purpose of the Komsomolsk – De Kastri Oil Product Pipeline Project is to transport oil products (i) Diesel Fuel 2.7 MTA, (ii) Naphtha 2.0 MTA and (iii) Jet Fuel 1.0 MTA produced in the Refinery Komsomolsk (located in Komsomolsk-on-Amur in Far East Russia) to other destinations in Far East Russia (Kamchatka, Chukchi Peninsula and Magadan) as well as to Pacific Rim Markets (China, Japan, Indonesia and possibly USA).

The current oil product transport scheme is from the Refinery Komsomolsk via railway to the Ports Vanino and Nakhodka. From there the oil products are delivered to Pacific Rim Markets by tankers. See figures below (blue lines). The new planned transport scheme replaces most of the existing railway transport volume so that most of the oil products are transported via pipeline (approx. 330 km) from the Refinery Komsomolsk to the Port De-Kastri. See figures below (red lines). The overall intent is to improve oil product transport reliability with the new system.

The new transportation system is planned to start operation by mid 2014 and foresees a period of operation of 30 years. Capital investment has been estimated in the order of 1 bn USD.

Design Institute “Nefteproduktprojekt”, a subsidiary of “Transnefteprodukt” which is itself a subsidiary of Russian Transneft, has previously performed the so-called Investment Justification work for the Project. This is somehow equivalent to the system engineering work usually performed during the Concept Selection facility lifecycle phase. This work has been carried out strictly following Russian norms and standards as is common practice in the Russian Federation. Design Institute has been appointed as the General Designer in the Project and has coordinated the Investment Justification work.

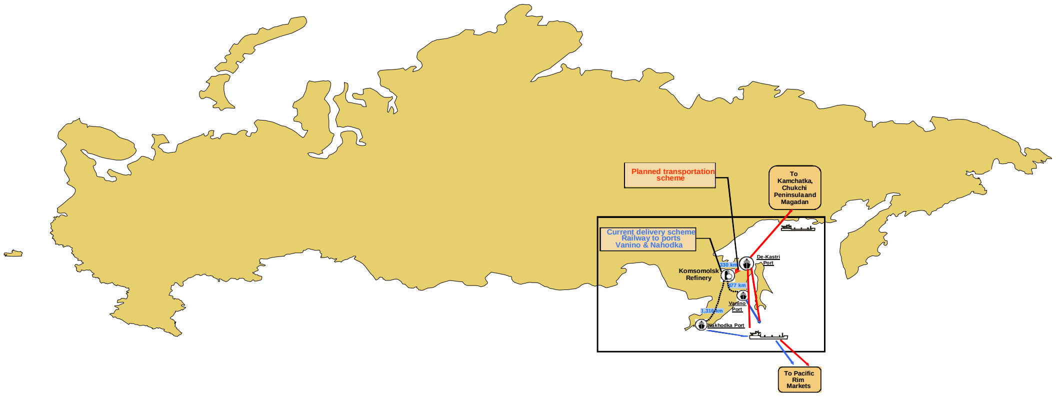

Planned transportation scheme
To Kamchatka, Chukchi Peninsula and Magadan
Current delivery scheme Railway to ports Vanino & Nahodka
Komsomolsk Refinery
De-Kastri Port
Vanino Port
Nakhodka Port
To Pacific Rim Markets

Figure 1: Oil Product Pipeline Komsomolsk-De Kastri Project – Overview location in the Russian Federation, adapted from [2]

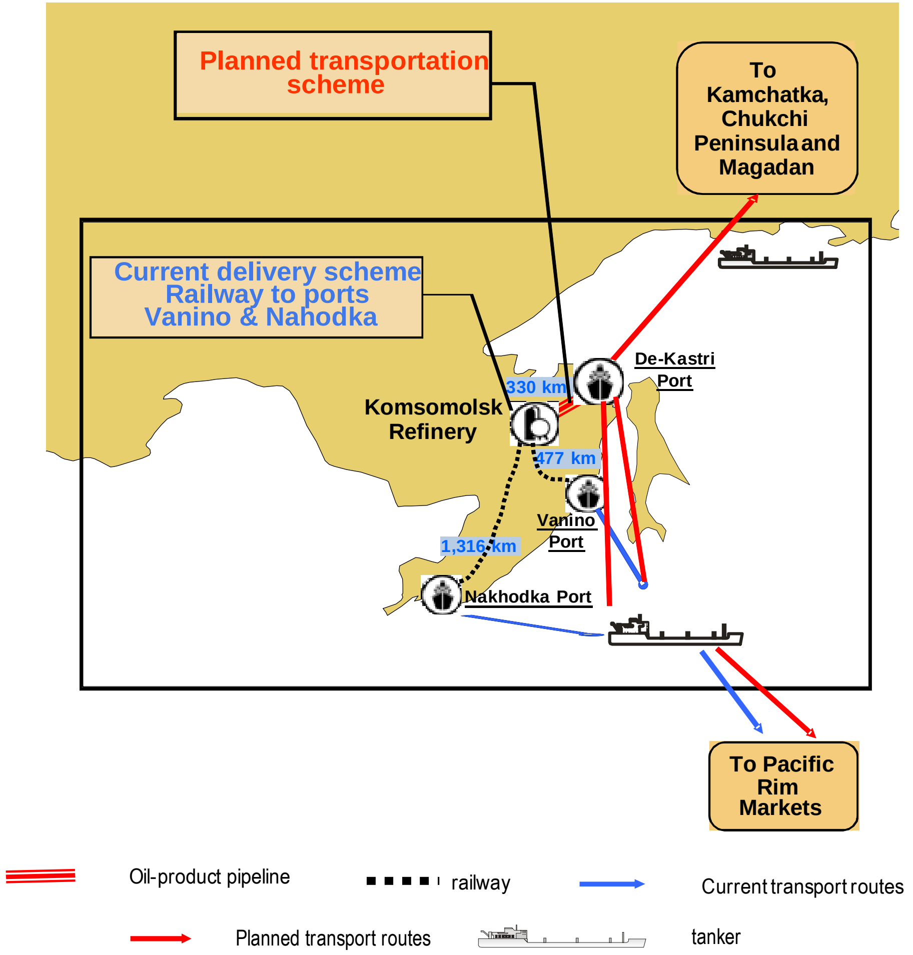


Figure 2: Oil Product Pipeline Komsomolsk-De Kastri Project – Detail current transportation scheme and planned transportation scheme, adapted from [2]

Before continuing with the Basic Design work on the basis of the results of the Investment Justification, Design Institute has contracted EC to perform Concept Selection and Functional Design according to international best practice. The intent of Design Institute with this contract is to try to find better solutions which will be compared with the solutions of the previous Investment Justification. The scope of the contract includes (i) System optimization and selection (pipeline, pump stations, tank farms, batch sizes, loading facilities and multiproduct technology), (ii) Preparation of Process Flow Diagrams and Piping and Instrumentation Diagrams (PIDs) as well as operating philosophies and (iii) Definition and specification of key equipment. The only planned "classic" Safety Study as per contract scope is a HAZOP after preparation of PIDs.

The figure below provides the System Flow Diagram inherited from the Investment Justification work performed by Design Institute.

The Pipeline System is divided in 3 Pipeline Sections:

- Pipeline Section I: from the existing Refinery fence to the fence of Head Tank Farm and Head Pump Station facilities.
- Pipeline Section II: from the fence of Head Tank Farm and Head Pump Station facilities to the fence of De-Kastri Tank Farm.
- Pipeline Section III: from the fence of De-Kastri Tank Farm to the offshore loading points.

The battery limit of the Project at the supply point is at the existing pump station located in the Refinery Komsomolsk, whose expansion requirement needs to be checked by EC (new Pipeline System replaces existing railway transport system, pumps could be re-used).

The battery limit of the Project at the delivery point is at the offshore loading points in the Port De-Kastri.

The system boundaries along the pipeline system are the fences of the facilities and the corridor or right of way of the pipeline and lines onshore and offshore.

2 Establishing the Goals of the System

The System Goals defined herein are considered as part of a Level 1 Intent Specification.

	System Goals for Project Example
G.1	*Transport and deliver oil products Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA from the Refinery Komsomolsk to tankers in Port De-Kastri.*
G.2	*Ensure quality of Oil Products to be delivered remains within specification.*
G.3	*Do not create unnecessary constraints to the tanker fleet operation.*
G.4	*Minimize the risk of losses to comply with high-level industry standards.*

Table 1: Example of System Goals defined for the Komsomolsk – De-Kastri Project

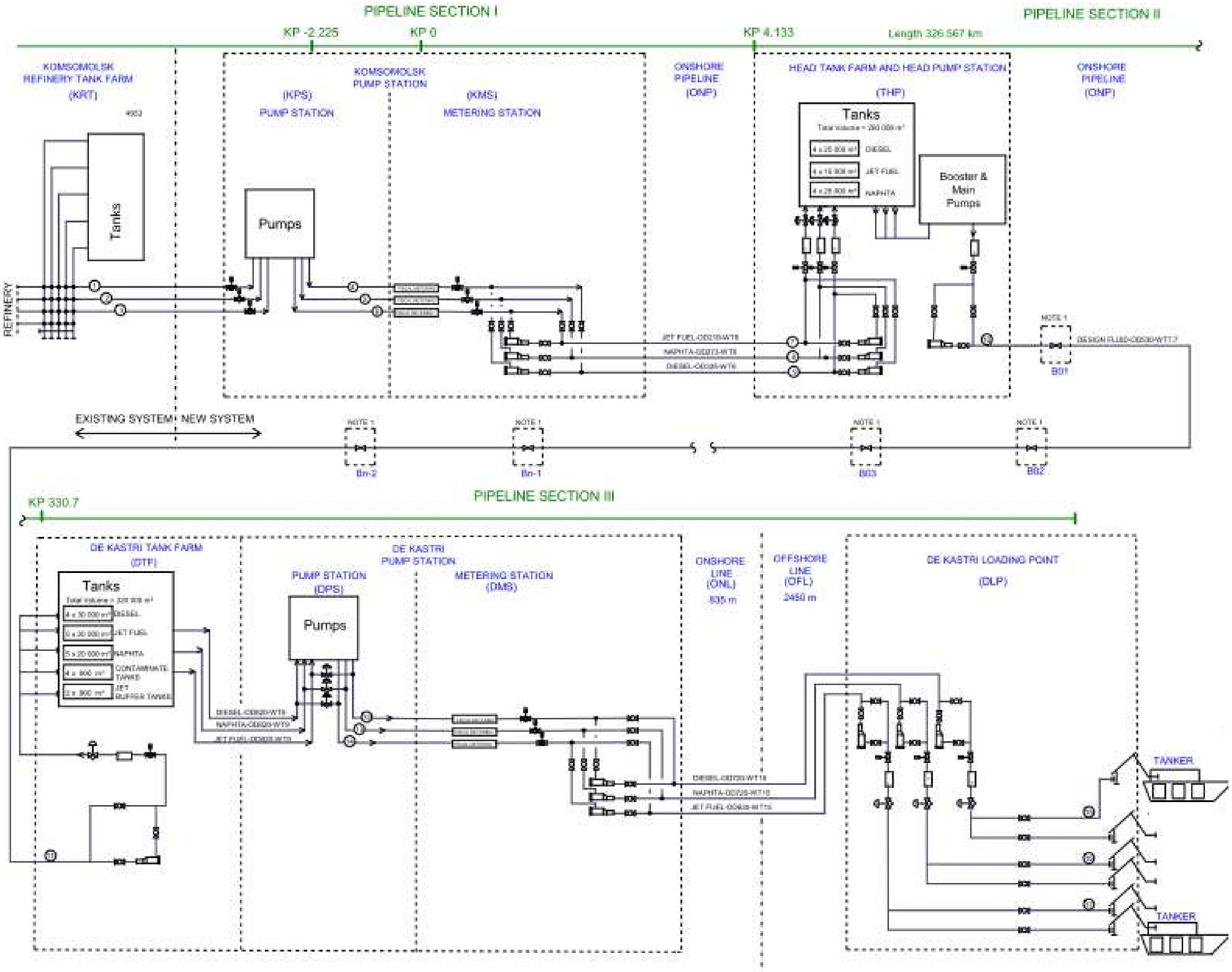


Figure 3: System Flow Diagram for the Komsomolsk – De-Kastri Project [17]

3 Defining Accidents

The following losses have been defined and are all considered unacceptable so that design should try to avoid or control them. No prioritization or rating of losses is performed for the purpose of this example in order not to increase complexity.

	Unacceptable Losses for Project Example
A.1	*Oil Products Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA cannot be transported and delivered. [G.1]*
A.2	*Oil Product tankers' schedules disrupted. [G.3]* **Rationale:** Even if overall the target yearly throughput is reached as per [G.1], individual tankers might have to wait for oil products during single operations, which might imply a disruption of the tanker schedule and might mean payment of demurrage costs.
A.3	*Quality of Oil Products delivered deviates from specification. [G.2]*
A.4	*Workforce or other stakeholders' fatality or permanent disability. [G.4]*
A.5	*Damage to the environment. [G.4]* **Assumption:** The environment is understood as the natural, industrial or social environment beyond the battery limits of the facilities and pipeline corridor (Right Of Way).
A.6	*Damage to pipeline system assets. [G.1], [G.2], [G.3], [G.4]* **Rationale:** Damage to the assets typically implies loss of production which depending on the magnitude of the loss may affect the target yearly throughput [G.1], the quality of the Oil Products transported [G.2] or the tankers schedule [G.3] too.

Table 2: Example of Unacceptable Losses defined for the Komsomolsk – De-Kastri Project

4 Identifying System Hazards

For the Project example the following system hazards have been identified.

	System Hazards for Project Example
H.1	*Pipeline System Blockage. [A.1], [A.2]*
H.2	*Oil Products cannot be delivered when required by tankers. [A.2]*
H.3	*Quality of Oil Products deviates from specification. [A.2], [A.3]*
H.4	*Fire and/ or explosion events. [A.4], [A.5], [A.6]* **Rationale:** Loss of Containment and product release which ignites.
H.5	*Spill to the environment. [A.5]* **Rationale:** Loss of Containment and product release which does not ignite, but which may contaminate the environment.

Table 3: Example of System Hazards identified for the Komsomolsk – De-Kastri Project

From these system hazards the following high-level safety constraints can be derived.

	High-level Safety Constraints for Project Example
SC.1	*Pipeline System must not block. [H.1]*
SC.2	*Oil Products must be ready for delivery when required by tankers. [H.2]*
SC.3	*Quality of Oil Products must not deviate from specification. [H.3]*
SC.4	*Fire and explosion events must be prevented. [H.4]*
SC.5	*Spills to the environment must be prevented. [H.5]*

Table 4: Example of High-level Safety Constraints derived for the Komsomolsk – De-Kastri Project

Strictly speaking in the frame of this thesis, SC.1, SC.2, SC.3 and SC.5 should be considered high-level design constraints, while SC.4 would be the only safety constraint according to the definition of safety provided above.

5 Integrating Safety into Architecture Selection and System Trade Studies

This step has not been developed for the Project Example. The reason why, as reported in the previous sections on current practice, is that safety is not systematically considered in the concept selection studies. During the concept selection phase of the "Oil Product Pipeline Komsomolsk – De-Kastri" three studies have been performed:

- Pipeline System Selection Study [11]
- Oil Product Logistic Transportation Model Study [12]
- Multiproduct Technology Study aiming to ensure Product Quality [13]

The following table maps the defined System Goals to the studies performed on which the concept selection decision is based.

Study performed for concept selection	**Related System Goal**
Pipeline System Selection Study [11]	G.1 "*Transport and deliver oil products Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA from the Refinery Komsomolsk to tankers in Port De-Kastri.*"
Oil Product Logistic Transportation Model Study [12]	G.1 "*Transport and deliver oil products Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA from the Refinery Komsomolsk to tankers in Port De-Kastri.*" G.3 "*Do not create unnecessary constraints to the tanker fleet operation.*"
Multiproduct Technology Study aiming to ensure Product Quality [13]	G.2 "*Ensure quality of Oil Products to be delivered remains within specification.*"

Table 5: Studies performed for concept selection of the Komsomolsk – De-Kastri Project mapped to defined System Goals

None of these studies is explicitly concerned with (i) ensuring safety as defined in goal G.4 "*Minimize the risk of losses to comply with high-level industry standards* or (ii) avoiding defined losses A.4 "*Workforce or other stakeholders' fatality or permanent disability*.

6 Documenting Environmental Assumptions

A so-called list of input data was prepared by the Project. This list contains besides confirmed data also assumptions. The list of input data was later transposed to a Basis of Design [14]. The table below shows some examples of the assumptions part of that Basis of Design.

	Some Assumptions for Project Example
EA.1	*There are no permafrost areas along the pipeline route.*
EA.2	*Burial depth to the center line of pipe is 1.5 m.*
EA.3	*Inlet fluid pressures at the battery limit with the Refinery Komsomolsk are Diesel 0.99 barg, Naphtha 1.01 barg and Jet A1 1.25 barg.*
EA.4	*Flashpoints of products received from the Refinery Komsomolsk are Diesel 67 deg C, Naphtha -25 deg C and Jet A1 38 deg C.*
EA.5	*Inlet fluid temperatures at the battery limit with the Refinery Komsomolsk are Diesel 5 deg C, Naphtha 5 deg C and Jet A1 5 deg C.*
EA.6	*System Operational Availability Factor is 93.20 %.*
EA.7	*Pump Efficiency is 85 %.*
EA.8	*Pumps' Mean Time Between Failures is 0.5 years.*
EA.9	*Maximum De-Kastri Port downtime due to bad weather conditions is 8 days.*
EA.10	*There is no fixed ice at De-Kastri Port during winter periods.*

Table 6: Examples of Assumptions identified for the Komsomolsk – De-Kastri Project [13], [14]

7 Generating System-Level Requirements

The main system goal is G.1 "*Transport and deliver oil products Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA from the Refinery Komsomolsk to tankers in Port De-Kastri"*.

Some of the system-level requirements (not safety-related) documented in the Project Basis of Design [14] are listed in the following table.

	Some System-Level Requirements for Project Example
1.1	*The pipeline system shall transport and deliver 5.7 MTA of oil products: Diesel Fuel 2.7 MTA, Naphtha 2.0 MTA and Jet A1 Fuel 1.0 MTA.*
1.2	*The pipeline system lifetime shall be 33 years.*
1.3	*The pipeline system shall transport the oil products by batching (consecutive pumping) using the direct contact method (without batch separation means).*
1.4	*The pipeline system operation mode shall be 365 days, 24 hours.*
1.5	*The pipeline system planned maintenance periods shall be every 3 years: 15 days of shutdown per year for 2 years and 45 days of shutdown per year for 1 year.*

Table 7: Examples of System-Level Requirements identified for the Komsomolsk – De-Kastri Project [14], [16]

8 Identifying High-Level Design and Safety Constraints

High-level safety constraints have been derived from the identified system hazards above:

- SC.1: *Pipeline System must not block. [H.1]*
- SC.2: *Oil Products must be ready for delivery when required by tankers. [H.2]*
- SC.3: *Quality of Oil Products must not deviate from specification. [H.3]*
- SC.4: *Fire and explosion events must be prevented. [H.4]*
- SC.5: *Spills to the environment must be prevented. [H.5]*

As remarked above, strictly speaking in the frame of this thesis, SC.1, SC.2, SC.3 and SC.5 should be considered high-level design constraints, while SC.4 would be the only safety constraint.

SC.1 and SC.2 can be refined considering the analysis performed in the Oil Product Logistic Transportation Model Study [12], for example:

- SC.1: *Pipeline System must not block. [H.1]*
    - *Sufficient equipment spare units must be provided to ensure continuation of system operation in the event of equipment breakdown.*
    - *Sufficient Oil Product stock in Head Tank Farm must be available to ensure continuation of system operation in the event of Refinery supply stoppage.*
- SC.2: *Oil Products must be ready for delivery when required by tankers. [H.2]*
    - *Stock available in the De-Kastri Tank Farm must be sufficient to fulfill demand of tankers waiting at the Port*

SC.3 can be refined considering the analysis performed in the Multiproduct Technology Study aiming to ensure Product Quality [13], for example:

- SC.3: *Quality of Oil Products must not deviate from specification. [H.3]*
  - *Jet A1 Fuel must be transported through pipeline section II between batches of Diesel Fuel only.*
  - *Naphtha must be transported between batches of Diesel Fuel only*
  - *Contaminate Mix of Jet A1 Fuel and Diesel Fuel must not be re-injected to Jet A1 Fuel.*

These refined constraints have been listed in the tables below as high-level operation and design constraints. It is however observed that the refinement of these constraints, originally derived as safety constraints from system goals and unacceptable losses, and overall the rationale to arrive to that refinement could probably be improved applying STPA techniques.

SC.4 and SC.5 have not been refined during the Conceptual Design work, as remarked above. SC.4 is addressed (refined) in the next section.

The following table lists examples of inherited constraints from the previous Investment Justification work which EC has to adhere to while developing the design of the Komsomolsk – De-Kastri Project.

	Some Inherited Design Constraints for Project Example	**Type**
C.1	*Investment costs must not exceed estimated CAPEX as in previous Investment Justification work.*	*Economic*
C.2	*System Operation Costs must not exceed estimated OPEX as in previous Investment Justification work.*	*Economic*
C.3	*Design must comply with VNTP-3-90 “Technological Engineering standards for branched pipelines; Instructions for technology of batch pumping of oil products through main oil product pipelines”.* **Rationale:** Design must comply with applicable Russian regulations. If the optimized design by EC proposes deviations, then these need to be negotiated with the relevant authorities.	*Norms and Standards*
C.4	*The pipeline system must follow the corridor of the existing pipelines “Okha – Komsomolsk-on-Amur” and “Sakhalin – Vladivostok”.*	*Route*
C.5	*Pipeline KP 0 must be located at Komsomolsk Metering Station (KMS)*	*Route*
C.6	*The pipeline system sections I and III must provide dedicated lines for the different oil products. (↓2.1, 2.2, 2.3, 2.5, 2.6, 2.7)*	*Design*
C.7	*The pipeline system must provide for a Tank Farm at the start of the pipeline section II for coping with fluctuations of supply.*	*Design*

	Some Inherited Design Constraints for Project Example	**Type**
C.8	*Head Tank Farm must be located at KP 4.133.*	*Route*
C.9	*The pipeline system must provide for a Tank Farm at the end of the pipeline section II for coping with fluctuations of demand.*	*Design*
C.10	*De-Kastri Tank Farm must be located at KP 330.*	*Route*
C.11	*De-Kastri Loading Point (DLP) must be located at KP 333.285.*	*Route*
C.12	*If an Intermediate Pump Station is required in pipeline section II, then a power generation plant with gas turbine must be provided.*	*Design*
C.13	*Pumps' drivers must be electrical motors for each pump station.*	*Design*
C.14	*Loading point type must be Arctic Loading Tower.*	*Design*
C.15	*Loading point must provide for 2 berths.*	*Design*

Table 8: Examples of Inherited Design Constraints identified for the Komsomolsk – De-Kastri Project [14]

The following table lists examples of operation constraints which have been identified for the design of the Komsomolsk – De-Kastri Project while performing trade studies.

	Some High-level Operation Constraints for Project Example
OP.1	*Jet A1 Fuel must be transported through pipeline section II between batches of Diesel Fuel only. (→Multiproduct Technology Study [13])*
OP.2	*Naphtha must be transported through pipeline section II between batches of Diesel Fuel only. (→Multiproduct Technology Study [13])*
OP.3	*Contaminate Mix of Jet A1 Fuel and Diesel Fuel must not be re-injected to Jet A1 Fuel. (→Multiproduct Technology Study [13])*
OP.4	*When tankers are waiting at the anchorage in Port De-Kastri, priority must be FIFO (First In First Out). (→Oil Product Transportation Study [12])*
OP.5	*A tanker must not be able to leave the berth while another tanker is approaching the berth. (→Oil Product Transportation Study [12])*
OP.6	*Pipeline Maximum Batch Size for oil products must be equal to the largest tanker size considered for that oil product: Diesel Fuel 105,000 m^3, Naphtha 66,000 m^3, Jet A1 Fuel 53,000 m^3. (→Oil Product Transportation Study [12])*
OP.7	*Tanker operations must be possible year-round. (→Oil Product Transportation Study [12])*
OP.8	*Tanker Port Turnaround time must not exceed 38 h in Spring-Summer period and 47 h in Fall-Winter period. (→Oil Product Transportation Study [12])*

	Some High-level Operation Constraints for Project Example
OP.9	*Simultaneous loading of 2 tankers must be possible. (→Oil Product Transportation Study [12])*
OP.10	*Planned Maintenance activities of De-Kastri Loading Point must be scheduled so as not to interfere with tankers' loading schedule. (→Oil Product Transportation Study [12])*

Table 9: Examples of High-level Operation Constraints identified for the Komsomolsk – De-Kastri Project [12], [13], [14]

The following table lists examples of high-level design constraints which have been identified for the design of the Komsomolsk – De-Kastri Project while performing trade studies.

	Some High-level Design Constraints for Project Example
C.16	*Minimum Pipe Wall Thickness in pipeline section I and II must be 6 mm. (→Pipeline System Selection Study [11])*
C.17	*Sufficient equipment spare units must be provided to ensure continuation of system operation in the event of equipment breakdown. (→Oil Product Transportation Study [12])*
C.18	*Sufficient Oil Product stock in Head Tank Farm must be available to ensure continuation of system operation in the event of Refinery supply stoppage. (→Oil Product Transportation Study [12])*
C.19	*Stock available in the De-Kastri Tank Farm must be sufficient to fulfill demand of tankers waiting at the Port. (→Oil Product Transportation Study [12])*
C.20	*Individual Tank Sizes in Tank Farms must be equal for a single oil product. (→Oil Product Transportation Study [12])*
C.21	*Tankers must not wait more than 12 h after acceptance of Notice Of Readiness by Port De-Kastri. (→Oil Product Transportation Study [12])*
C.22	*Filling and emptying of individual Tanks in Tank Farms at the same time must not be possible. (→Oil Product Transportation Study [12])*
C.23	*Contamination of Jet A1 Fuel must not be allowed. (→Multiproduct Technology Study [13], ↓2.20)*
C.24	*Actual Oil Product Mix Zone Length must not be greater than Calculated Oil Product Mix Zone Length. (→Multiproduct Technology Study [13], ↓OP.16, L3)*
C.25	*Flash Point of delivered Jet A1 Fuel must not be lower than specified. (→Multiproduct Technology Study [13])*
C.26	*Freezing Point of delivered Jet A1 Fuel must not be lower than specified. (→Multiproduct Technology Study [13])*
C.27	*Sulphur Content of delivered Diesel Fuel must not be higher than specified. (→Multiproduct Technology Study [13])*
C.28	*Flash Point of delivered Diesel Fuel must not be lower than specified. (→Multiproduct Technology Study [13])*
C.29	*Naphtha delivered must not contain traces of water. (→Multiproduct Technology Study [13])*

	Some High-level Design Constraints for Project Example
C.30	*Boiling Point of Naphtha delivered must not be higher than specified. (→Multiproduct Technology Study [13])*

Table 10: Examples of High-level Design Constraints identified for the Komsomolsk – De-Kastri Project [11], [12], [13]

9 Performing System Design and Analysis

Although the initial scope of work of EC in this Project Example included performing a HAZOP after preparation of PIDs, the project management team (formed by EC and the direct client Design Institute) has decided to exclude this activity due to schedule and budget constraints.

In the following paragraphs, first examples of lower-level operation requirements and design constraints as well as design features (Level 2 intent specification), also derived in the frame of the trade studies referred in the precious points, are provided. The second part of this point focuses on refining the high-level safety constraint SC.4: "*Fire and explosion events must be prevented"* by applying STPA and comparing results to the safety-related design features proposed for the Komsomolsk – De-Kastri Project.

9.1 Examples of lower-level requirements, design constraints and design features

The following table lists examples of lower-level operation requirements and design constraints which have been derived for the design of the Komsomolsk – De-Kastri Project while performing trade studies.

	Some Lower Level Operation Requirements and Design Constraints for Project Example
OP.11	*Contaminate Mix Zone of Diesel Fuel and Naphtha must be divided in 2 parts of equal volume at the middle of the mixing zone. The first part must be routed to a first contaminate tank (Naphtha Diesel Mix) and the second part must be routed to a second contaminate tank (Diesel Naphtha Mix) (→Multiproduct Technology Study [13], ↓2.19)*
OP.12	*The mixture in the Naphtha Diesel Contaminate Tank must be re-injected into the Naphtha stream for export. The mixture in the Diesel Naphtha Contaminate Tank must be re-injected into the Diesel stream. (→Multiproduct Technology Study [13])*
OP.13	*Contaminate Mix Zone of Diesel Fuel and Jet A1 Fuel must be divided in 2 parts of equal volume at the middle of the mixing zone. The first part must be routed to a first contaminate tank (Jet A1 Diesel Mix) and the second part must be routed to a second contaminate tank (Diesel Jet A1 Mix) (→Multiproduct Technology Study [13], ↓2.19)*
OP.14	*The mixture in the Jet A1 Diesel Contaminate Tank must be re-injected into the Diesel stream. (→Multiproduct Technology Study [13])*

	Some Lower Level Operation Requirements and Design Constraints for Project Example
OP.15	*A part of the mixture in the Diesel Jet A1 Contaminate Tank must be re-injected into the Naphtha stream, while the other part must be re-injected into the Diesel stream. The specific quantities shall be specified by the Operator. (→Multiproduct Technology Study [13])*
OP.16	*Main Head Pumps shall pump the largest possible batch of a single oil product. (→Oil Product Transportation Study [12], ↑C.24)*
OP.17	*Main Head Pumps shall pump a batch of the required oil product according to demand forecast. (→Oil Product Transportation Study [12])*
OP.18	*De-Kastri Port shall not follow a Spot-Selling policy, but a Scheduled-Selling policy. (→Oil Product Transportation Study [12]*
OP.19	*A Stand Still time of 6 hours must be allowed for Tanks in De Kastri tank farm only between end of tank filling and beginning of tanker loading (→Oil Product Transportation Study [12])*
OP.20	*A Settling time of 24 hours must be allowed for Jet A1 Tanks in De Kastri tank farm only between end of Stand Still time and beginning of tanker loading (→Oil Product Transportation Study [12])*

Table 11: Examples of Lower-level Operation Constraints derived for the Komsomolsk – De-Kastri Project [12], [13]

The following table lists examples of design features which have been derived for the design of the Komsomolsk – De-Kastri Project while performing trade studies.

	Some Design Features for Project Example
2.1	*The pipeline system section I Diesel Fuel line shall provide Outer Diameter (OD) 273 mm and Wall Thickness (WT) 6 mm. (→Pipeline System Selection Study [11], ↑C.6)*
2.2	*The pipeline system section I Naphtha line shall provide Outer Diameter (OD) 245 mm and Wall Thickness (WT) 6 mm. (→Pipeline System Selection Study [11], ↑C.6)*
2.3	*The pipeline system section I Jet A1 Fuel line shall provide Outer Diameter (OD) 178 mm and Wall Thickness (WT) 6 mm. (→Pipeline System Selection Study [11], ↑C.6)*
2.4	*The pipeline system section II shall provide Outer Diameter (OD) 530 mm and Wall Thickness (WT) 7.72 mm. (→Pipeline System Selection Study [11], ↓L1, L4)*
2.5	*The pipeline system section III Diesel Fuel line shall provide Outer Diameter (OD) 720 mm. (→Pipeline System Selection Study [11], ↑C.6)*
2.6	*The pipeline system section III Naphtha line shall provide Outer Diameter (OD) 720 mm. (→Pipeline System Selection Study [11], ↑C.6)*

	Some Design Features for Project Example
2.7	*The pipeline system section III Jet A1 Fuel line shall provide Outer Diameter (OD) 630 mm. (→Pipeline System Selection Study [11], ↑C.6)*
2.8	*Head Tank Farm Total Nominal Volume shall be 280 000 m³. (→Oil Product Transportation Study [12])*
2.9	*Diesel Fuel Flowrate in pipeline system section I shall be 372 m^3/h. (→Oil Product Transportation Study [12])*
2.10	*Naphtha Flowrate in pipeline system section I shall be 314 m^3/h. (→Oil Product Transportation Study [12])*
2.11	*Jet A1 Fuel Flowrate in pipeline system section I shall be 141 m^3/h. (→Oil Product Transportation Study [12])*
2.12	*Head Tank Farm Diesel Fuel configuration shall be 4 tanks of nominal volume 25,000 m^3/each. (→Oil Product Transportation Study [12])*
2.13	*Head Tank Farm Naphtha configuration shall be 4 tanks of nominal volume 25,000 m^3/each. (→Oil Product Transportation Study [12])*
2.14	*Head Tank Farm Jet A1 Fuel configuration shall be 4 tanks of nominal volume 20,000 m^3/each. (→Oil Product Transportation Study [12])*
2.15	*De-Kastri Tank Farm Total Nominal Volume shall be 320 000 m³. (→Oil Product Transportation Study [12])*
2.16	*De-Kastri Tank Farm Diesel Fuel configuration shall be 4 tanks of nominal volume 30,000 m^3/each. (→Oil Product Transportation Study [12])*
2.17	*De-Kastri Tank Farm Naphtha configuration shall be 5 tanks of nominal volume 20,000 m^3/each. (→Oil Product Transportation Study [12])*
2.18	*De-Kastri Tank Farm Jet A1 Fuel configuration shall be 5 tanks of nominal volume 20,000 m^3/each. (→Oil Product Transportation Study [12])*
2.19	*De-Kastri Tank Farm shall provide 4 Contaminate Tanks of nominal volume 900 m^3/each. (→Multiproduct Technology Study [13], ↑OP.11, OP.13)* **Assumption:** Mixing zone volumes are expected in the order of magnitude of 300 m^3 each. Each mixing zone is routed into 2 contaminate tanks (150 m^3 each as dedicated mixing zone). Each contaminate tank is assumed to be able to handle 6 dedicated mixing zones. This figure takes into account the scenario in which some unexpected events would prevent re-injection.
2.20	*De-Kastri Tank Farm shall provide 2 Jet A1 Fuel Buffer Tanks of nominal volume 900 m^3/each. (→Multiproduct Technology Study [13], ↑C.23)* **Assumption:** Buffer batches are assumed in the order of magnitude of 300 m^3 each. Each buffer tank is assumed to be able to handle 3 buffer batches.

Table 12: Examples of Design Features identified for the Komsomolsk – De-Kastri Project [11], [12], [13]

9.2 STPA for refining SC.4: “Fire and explosion events must be prevented”

The following analysis is based on typical pipeline system control principles documented:

- Specifically for the “Oil Product Pipeline Komsomolsk – De-Kastri” in the “Operation and Control Philosophy” [18].
- Generally for other pipeline systems such as the “Burgas-Alexandroupolis Crude Oil Pipeline Project” in “Overall Operating and Control Concept” [19] and “Operating and Control Philosophy” [20].

The control principles and information used herein are not complete and might deviate from the latest Project specific decisions taken about operations (e.g. a significant uncertainty during the design process is who will be the operator of the pipeline system. Here it is assumed that a different organization –not the Komsomolsk Refinery– will be the operator). The analysis below is only intended for illustration of what can be done and how the techniques can help.

9.2.1 Brief description of Concept of Operations

The purpose of the Komsomolsk – De Kastri Oil Product Pipeline Project is to transport oil products (i) Diesel Fuel, (ii) Naphtha and (iii) Jet Fuel produced in the Refinery Komsomolsk to other destinations in Far East Russia, as well as to Pacific Rim Markets.

For this purpose the pipeline system foresees the following installations as illustrated in Figure 4:

- Pumping station and metering system in the Komsomolsk Refinery area,
- Dedicated lines, one per product, from Komsomolsk Refinery to THP of approximately 6.4 kilometers,
- Head tank farm and Pump Station,
- Cross-country multiproduct pipeline of approximately 326.6 kilometers,
- De-Kastri Export Terminal including a Tank Farm, loading pumps, a metering system, dedicated loading lines of approximately 3.3 kilometers and a sea island loading point for tanker loading operations.

The system flow diagram provided in Figure 4 can be simplified as illustrated in the block diagram of Figure 5.

9.2.2 Preliminary System Control Structure

Pipeline system control is basically carried out at two levels:

- At System level (remotely from a Main Control Centre, MCC),
- At Station level, which actually means at location level because Local Control Centers (LCC) are provided in the different locations (e.g. LCC at the Head Facilities controls the processes in the tank farm and in the pump station).

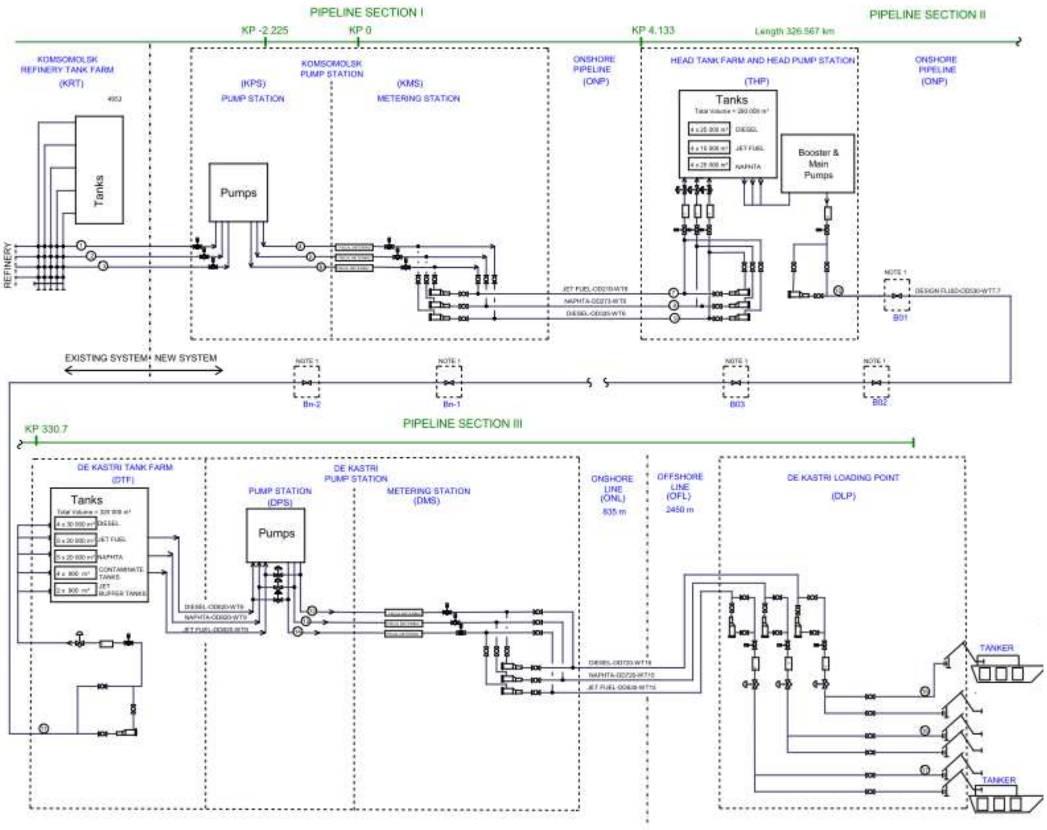


Figure 4: Revised System Flow Diagram of “Oil Product Pipeline Komsomolsk – De-Kastri” [17]

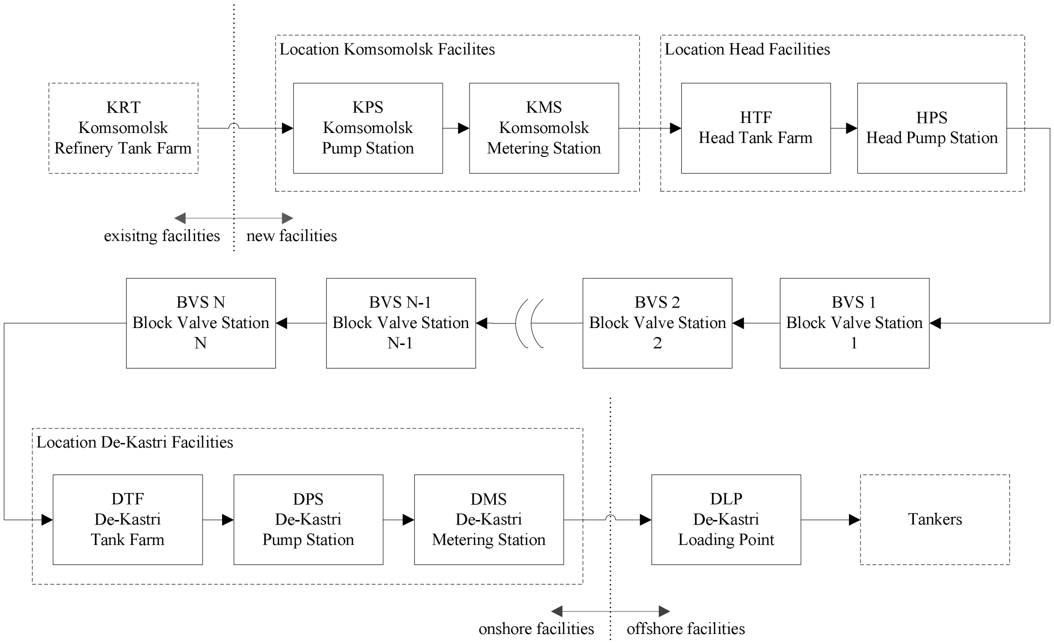


Figure 5: Simplified System Block Diagram for “Oil Product Pipeline Komsomolsk – De-Kastri”

Typical safety-critical systems foreseen for control of fire and explosion hazards in pipeline systems are:

- At System level:
    - Leak Detection System (LDS),
    - Emergency Shut Down System (ESD) push button to initiate Local ESDs. Automatic procedure initiated remotely by operator at MCC. The purpose of the ESD System is to shut down units or stations in safety-critical situations.
    - Controlled Operation ESD (COESD) for the whole system (e.g. in case of confirmed leak detection along the pipeline system). Manual procedure executed remotely by operator at MCC.
- At Station level (Integrated Control and Safety System (ICSS)):
    - Station Control System (SCS)
        - Pressure Control System
        - Leak Detection System (LDS)
    - Emergency Shut Down System (ESD). Automatic procedure initiated either automatically or by operator via push down button.
    - Fire and Gas Detection System (F&G)

      The purpose of the F&G System is to detect flammable gases, smoke and heat within the shelters and compounds in the pipeline system.
    - Fire Fighting System (only in some stations/ locations)
    - Intrusion Detection System

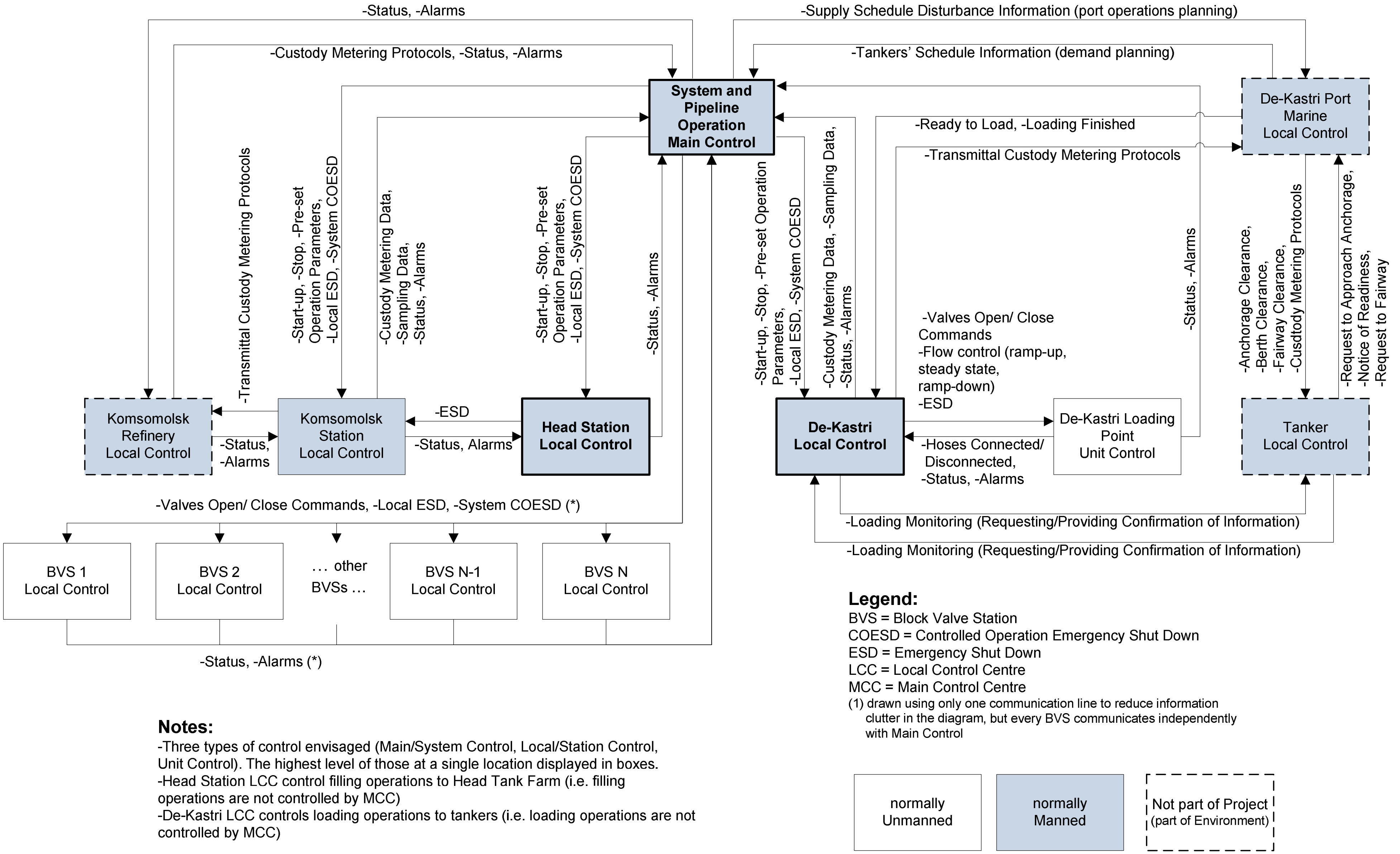
The fire and explosion hazard control systems listed above are typically classified as:

- Prevention (ESD, Pressure Control System and Flow Path Supervision System),
- Detection (LDS, F&G, Intrusion Detection System),
- Mitigation –protection– (ESD, Fire Fighting System, COESD).

The high-level system control structure is provided in Figure 6.

The normal system operation mode is the “Pipeline Automatic Mode” which is the control mode with the highest level of automation. System and pipeline control is performed from the MCC. Basically the MCC starts the automatic programs which manage the Local Controls at the different locations/ stations:

- The MCC interfaces with the external control units (i.e. controllers not part of the new transportation system), which are (i) the “Refinery Komsomolsk LCC” upstream and (ii) the “De-Kastri Port Marine Control Centre” downstream.


-Status, -Alarms
-Custody Metering Protocols, -Status, -Alarms
-Supply Schedule Disturbance Information (port operations planning)
-Tankers' Schedule Information (demand planning)
System and Pipeline Operation Main Control
De-Kastri Port Marine Local Control
-Ready to Load, -Loading Finished
-Transmittal Custody Metering Protocols
-Transmittal Custody Metering Protocols
-Start-up, -Stop, -Pre-set Operation Parameters, -Local ESD, -System COESD
-Custody Metering Data, -Sampling Data, -Status, -Alarms
-Start-up, -Stop, -Pre-set Operation Parameters, -Local ESD, -System COESD
-Status, -Alarms
-Start-up, -Stop, -Pre-set Operation Parameters, -Local ESD, -System COESD
-Custody Metering Data, -Sampling Data, -Status, -Alarms
-Valves Open/ Close Commands
-Flow control (ramp-up, steady state, ramp-down)
-ESD
-Status, -Alarms
-Anchorage Clearance, -Berth Clearance, -Fairway Clearance, -Cusdtody Metering Protocols
-Request to Approach Anchorage, -Notice of Readiness, -Request to Fairway
Komsomolsk Refinery Local Control
-Status, -Alarms
Komsomolsk Station Local Control
-ESD
-Status, Alarms
Head Station Local Control
De-Kastri Local Control
De-Kastri Loading Point Unit Control
-Hoses Connected/ Disconnected, -Status, -Alarms
Tanker Local Control
-Valves Open/ Close Commands, -Local ESD, -System COESD (*)
-Loading Monitoring (Requesting/Providing Confirmation of Information)
-Loading Monitoring (Requesting/Providing Confirmation of Information)
BVS 1 Local Control
BVS 2 Local Control
… other BVSs …
BVS N-1 Local Control
BVS N Local Control
-Status, -Alarms (*)

Legend:
BVS = Block Valve Station
COESD = Controlled Operation Emergency Shut Down
ESD = Emergency Shut Down
LCC = Local Control Centre
MCC = Main Control Centre
(1) drawn using only one communication line to reduce information clutter in the diagram, but every BVS communicates independently with Main Control

□ normally Unmanned
▨ normally Manned
⬚ Not part of Project (part of Environment)

Notes:
-Three types of control envisaged (Main/System Control, Local/Station Control, Unit Control). The highest level of those at a single location displayed in boxes.
-Head Station LCC control filling operations to Head Tank Farm (i.e. filling operations are not controlled by MCC)
-De-Kastri LCC controls loading operations to tankers (i.e. loading operations are not controlled by MCC)

Figure 6: High-Level System Control Structure of "Oil Product Pipeline Komsomolsk – De-Kastri".

  - The Refinery LCC and the MCC exchange information about status and alarms in their facilities, but none can initiate ESD actions on the facilities of the other. The Refinery Komsomolsk owns the products transported and the booster pump station, metering and sampling station located in the "Komsomolsk Station", see Figure 5. That is why the Custody Metering Protocols are issued by the Refinery Komsomolsk to the MCC (i.e. to the pipeline operator).
  - Planning information as well as notification of production disturbances are exchanged between the MCC and the Port Control. This is a control on a very high level and on a monthly/ weekly basis (i.e. high-level transportation system scheduling).
- The MCC provides commands to the Local Controls for:
  - Start-up and stop operations (e.g. flow increase/ decrease),
  - Pre-set of process parameters (e.g. pump stations flowrate or suction pressure at pump stations),
  - Remote control of equipment changeover at the locations (e.g. between essential equipment groups such as pump trains or metering trains),
  - Initiation of Local automatic ESD actions in the different locations as well as manually Controlled Operation ESD (COESD) for the whole system (e.g. in case of confirmed leak detection along the pipeline system).

  The MCC also receives information from the Local Controls on status of equipment and process parameters, as well as alarms.
- The MCC remotely controls the pipeline and its Block Valve Stations (BVS), receiving back information on status of equipment and process parameters, as well as alarms.

Station/ Local Control is performed from the different LCCs. These interface mainly with the MCC, but some can also interface with other Local Controls as for the case of the "Head LCC" and the "De-Kastri LCC". For example, the "De-Kastri LCC" performs the control of the loading operations. These two LCCs also perform very important controls at the station level like the tank farms control and the product quality control. These are not illustrated in Figure 6.

Between the safety-critical systems listed above, the ESD System has been selected for further analysis because it is one of the systems on which project teams over-rely and focus the most during the SIL Assessments (i.e. "the ESD System will prevent all kinds of hazards when others have failed to do so").

There are typically four ESD-levels:

- ESD-Level 1: Overall System Shutdown

  (This is normally not envisaged for this type of systems)
- ESD-Level 2: Multiple Station Shutdown

  (Initiation of Local automatic ESD actions, possible from MCC only)
  - Loading Operation Shut Down
  - Main Pipeline Shut Down
  - Filling Operation Shut Down

- ESD-Level 3: Single Station Shutdown

  (Initiation of Local automatic ESD actions, possible (i) automatically by ESD System, (ii) remotely from MCC, (iii) locally from LCC and (iv) manually in the field –ESD push buttons–)

  - Komsomolsk Station
  - Head Station
  - BVSs
  - De-Kastri Station

  ESD-Level 3 actions at Head Station and De-Kastri Station include: (i) Trip Pump, (ii) Close Station Inlet/ Outlet ESD Valves, (iii) Isolate Tanks and (iv) Trip Upstream Pumps.

- ESD-Level 4: Part/section of a Station Shutdown

  (Initiation of Local automatic ESD actions, possible (i) automatically by ESD System, (ii) remotely from MCC, (iii) locally from LCC and (iv) manually in the field –ESD push buttons–)

  ESD-Level 4 actions trigger only Pump Trip.

The system control structure presented in Figure 7 illustrates the ESD control in one general station/ location and the interface with the MCC and the controlled process. Examples of loops triggering ESD-Level 3 and ESD-Level 4 have been illustrated. For simplification purposes no control actions have been displayed to/ from interfacing stations/ LCCs, although the "Head LCC" and the "De-Kastri LCC" execute some, as explained above. In "Pipeline Automatic Mode" steady-state operation, intervention from the operators is not envisaged, except by using the shut down push buttons in case of emergency, which triggers the Local ESDs. The control structure of Figure 7 displays the safety-critical systems listed above and their interfaces to the ESD system. Only some examples of signals triggering ESD-Level 3 and Level 4 actions have been provided. The details of Figure 7 are self-explanatory.

9.2.3 Hazard Analysis and Generation of Safety Requirements and Constraints

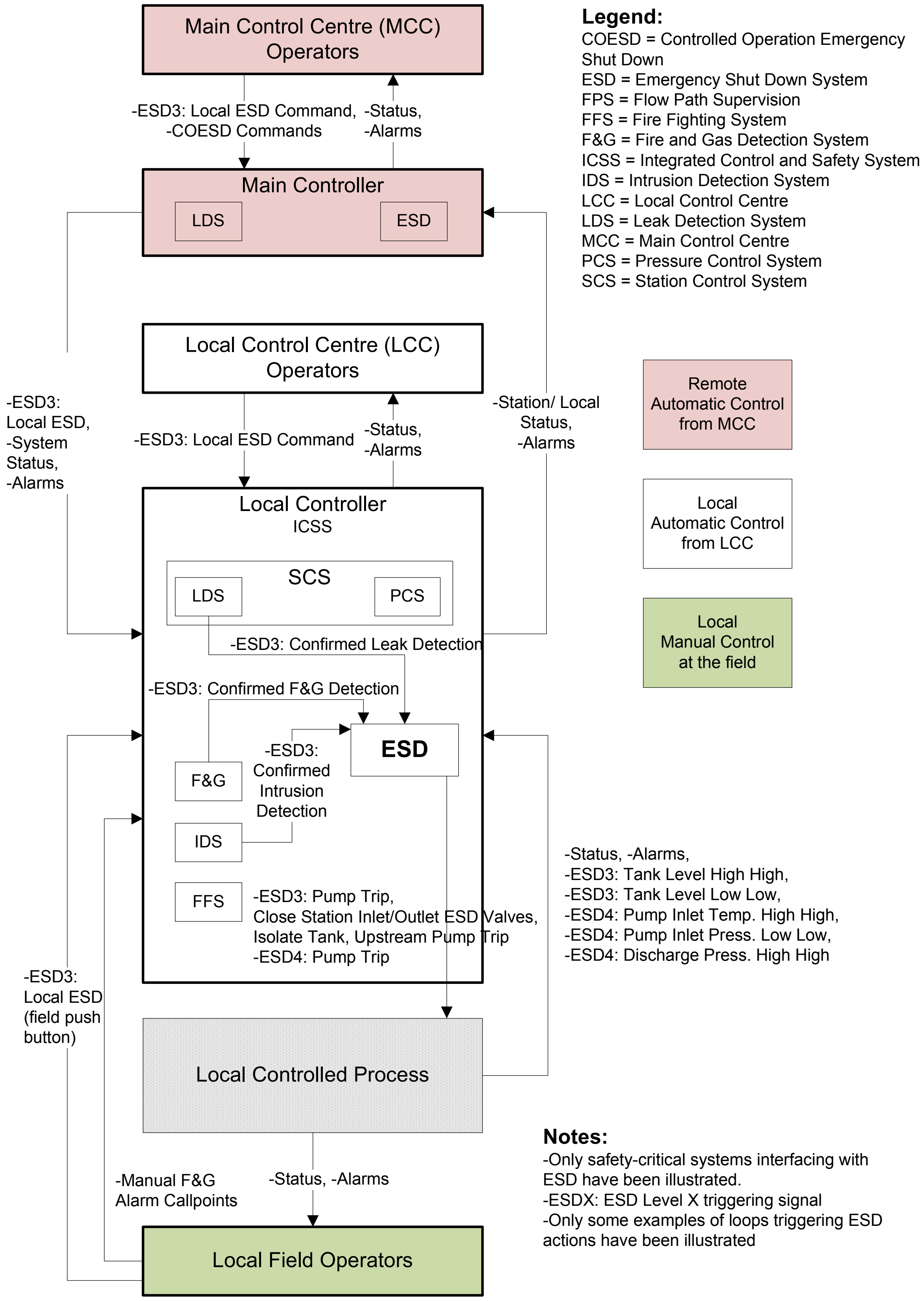
The high-level hazard of concern in this analysis is:

SC.4: *"Fire and/ or explosion events"*

9.2.3.1 Identifying Unsafe Control Actions (UCAs)

The first step of STPA, once a control structure is characterized, is to identify possible Unsafe Control Actions the controllers might execute. According to Figure 7, there are five controllers who can trigger and/ or execute ESD actions:

- Operators in MCC (Human Controllers)
- Main Controller (Automated Controller)
- Operators in LCC (Human Controllers)
- Local Controller (Automated Controller)
- Operators in the field (Human Controllers)


Main Control Centre (MCC) Operators
-ESD3: Local ESD Command,
-COESD Commands
-Status,
-Alarms
Main Controller
LDS
ESD
Local Control Centre (LCC) Operators
-ESD3:
Local ESD,
-System
Status,
-Alarms
-ESD3: Local ESD Command
-Status,
-Alarms
-Station/ Local
Status,
-Alarms
Remote Automatic Control from MCC
Local Automatic Control from LCC
Local Manual Control at the field
Local Controller
ICSS
SCS
LDS
PCS
-ESD3: Confirmed Leak Detection
-ESD3: Confirmed F&G Detection
ESD
F&G
-ESD3:
Confirmed
Intrusion
Detection
IDS
FFS
-ESD3: Pump Trip,
Close Station Inlet/Outlet ESD Valves,
Isolate Tank, Upstream Pump Trip
-ESD4: Pump Trip
-Status, -Alarms,
-ESD3: Tank Level High High,
-ESD3: Tank Level Low Low,
-ESD4: Pump Inlet Temp. High High,
-ESD4: Pump Inlet Press. Low Low,
-ESD4: Discharge Press. High High
-ESD3:
Local ESD
(field push
button)
Local Controlled Process
-Manual F&G
Alarm Callpoints
-Status, -Alarms
Local Field Operators

Legend:
COESD = Controlled Operation Emergency Shut Down
ESD = Emergency Shut Down System
FPS = Flow Path Supervision
FFS = Fire Fighting System
F&G = Fire and Gas Detection System
ICSS = Integrated Control and Safety System
IDS = Intrusion Detection System
LCC = Local Control Centre
LDS = Leak Detection System
MCC = Main Control Centre
PCS = Pressure Control System
SCS = Station Control System

Notes:
-Only safety-critical systems interfacing with ESD have been illustrated.
-ESDX: ESD Level X triggering signal
-Only some examples of loops triggering ESD actions have been illustrated

Figure 7: Pipeline System ESD Control Structure for a General Station of "Oil Product Pipeline Komsomolsk – De-Kastri"

The following analysis will focus on the Local Controller, which as displayed in Figure 7, is responsible for a good part of the processing of safety-critical signals and execution of actions. Table 14 identifies Unsafe Control Actions by the Local Controller. This table has been generated following the methodology explained in Chapters 4 and 8 of Leveson's "Engineering a Safer World" [1] which is based on the fact that control actions can be hazardous in four ways:

- A control action required for safety is not provided or not followed.
- An Unsafe Control Action is provided that leads to a hazard.
- A potentially safe control action is provided too late, too early, or out of sequence.
- A safe control action is stopped too soon or applied too long (for a continuous or non-discrete control action).

Eleven (11) Unsafe Control Actions have been identified.

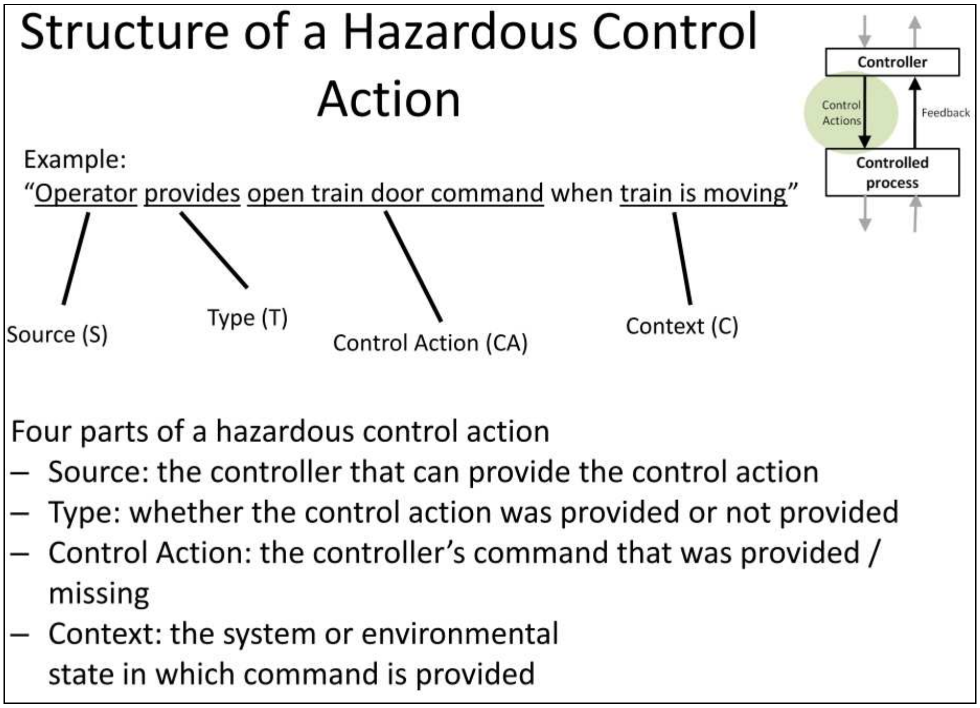
	Unsafe Control Actions of Local Controller on ESD Procedures
UCA-LC.1	ESD3 actions not provided when required.
UCA-LC.2	ESD3 actions provided, but executing in the wrong components.
UCA-LC.3	ESD3 actions provided too late.
UCA-LC.4	ESD3 actions provided out of sequence.
UCA-LC.5	ESD3 actions provided, but stopped too early.
UCA-LC.6	ESD4 actions not provided.
UCA-LC.7	ESD4 actions provided too late.
UCA-LC.8	ESD4 actions provided out of sequence.
UCA-LC.9	ESD4 actions provided, but stopped too early.
UCA-LC.10	Confirmed leak detection or confirmed fire or gas detection or confirmed intrusion detection not provided. **Remark:** This should be broken into 3 SCs in real life.
UCA-LC.11	Confirmed leak detection or confirmed fire or gas detection or confirmed intrusion detection provided too late. **Remark:** This should be broken into 3 SCs in real life.

Table 13: List of identified Unsafe Control Actions of Local Controller on ESD procedures in a General Station of "Oil Product Pipeline Komsomolsk – De-Kastri"

These Unsafe Control Actions should be translated into safety constraints on the Local Controller. In order to generate more precise safety constraints (e.g. not only specifying "ESD3 actions must be provided when required"), the "Structure of Hazardous Control Actions" proposed by Thomas would help. See Figure 8 below.

Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Wrong Timing/ Order Causes Hazard**	**Stopped Too Soon or Applied Too Long Causes Hazard**
STPA-LC.1 **ESD3: Pump Trip, Close Station Inlet/ Outlet Valves, Isolate Tanks, Upstream Pump Trip**	Not providing would lead to a major accident because the quantities of hydrocarbon released would be very high and active and passive protecting systems would not cope with the fires generated evolving into a major explosion – unsafe	-Providing when not required basically would only lead to loss of operation – not unsafe -Providing confusing valves to close, for example, could lead to overpressures potentially causing LOC – unsafe	-Providing too early would only lead to loss of operation – not unsafe -Providing too late might allow enough time for formation of flammable mixture and ignition – unsafe -Providing out of sequence (e.g. close station inlet/ outlet before tripping pump) would lead to overpressures potentially causing LOC – unsafe	-Interrupting pump trips or leaving valves partially open would allow for formation of flammable mixture and ignition – unsafe -Providing too long not relevant – not unsafe
STPA-LC.2 **ESD4: Pump Trip**	Not providing might cause cavitation in the pumps and eventually overpressures potentially causing LOC – unsafe	Providing when not required basically would only lead to loss of operation – not unsafe	-Providing too early would only lead to loss of operation – not unsafe -Providing too late might cause cavitation in the pumps and eventually overpressures potentially causing LOC – unsafe -Providing out of sequence (i.e. wrong order in pump trip steps) might lead to cavitation in the pumps and eventually overpressures potentially causing LOC – unsafe	Interrupting pump trips might lead to cavitation in the pumps and eventually overpressures potentially causing LOC – unsafe -Providing too long not relevant – not unsafe
STPA-LC.3 **Confirmed Leak or F&G or Intrusion Detection to initiate ESD3**	Not providing would cause formation of flammable mixture and ignition – unsafe **Assumption:** intruders' objective is to perform hot-tap and steal products for re-selling.	Providing when not required basically would only lead to loss of operation – not unsafe	-Providing too early would only lead to loss of operation – not unsafe -Providing too late might allow enough time for formation of flammable mixture and ignition – unsafe -Providing out of sequence not relevant (discrete events) – not unsafe	Not relevant (discrete events) – not unsafe

Table 14: Unsafe Control Actions of Local Controller on ESD procedures in a General Station of "Oil Product Pipeline Komsomolsk – De-Kastri"



Structure of a Hazardous Control Action

Example:
"Operator provides open train door command when train is moving"

Four parts of a hazardous control action

- Source: the controller that can provide the control action
- Type: whether the control action was provided or not provided
- Control Action: the controller's command that was provided / missing
- Context: the system or environmental state in which command is provided

Figure 8: Structure of a Hazardous Control Action [22]

This way for example UCA-LC.1 "ESD3 actions not provided when required" would be translated into the following UCAs which have been derived by observing Figure 7:

	Unsafe Control Actions derived from UCA-LC.1
UCA-LC.1-1	Local Controller does not provide ESD3 Control Actions when Tank Level has reached High High.
UCA-LC.1-2	Local Controller does not provide ESD3 Control Actions when Tank Level has reached Low Low.
UCA-LC.1-3	Local Controller does not provide ESD3 Control Actions when Confirmed Leak Detection.
UCA-LC.1-4	Local Controller does not provide ESD3 Control Actions when Confirmed Fire or Gas Detection.
UCA-LC.1-5	Local Controller does not provide ESD3 Control Actions when Confirmed Intrusion Detection.
UCA-LC.1-6	Local Controller does not provide ESD3 Control Actions when Local Operator has pushed ESD push button in the field.
UCA-LC.1-7	Local Controller does not provide ESD3 Control Actions when Local Operator has pushed ESD push button in the LCC.
UCA-LC.1-8	Local Controller does not provide ESD3 Control Actions when Main Controller has provided Local ESD Command.

Table 15: List of Unsafe Control Actions derived from UCA-LC.1 "ESD3 actions not provided when required" in a General Station of "Oil Product Pipeline Komsomolsk – De-Kastri"

Then the safety-constraints generated would be much more precise and complete:

	Safety-Constraints generated from UCA-LC.1
SC-LC.1	Local Controller must provide ESD3 Control Actions when Tank Level has reached High High. (→STPA-LC.1)
SC-LC.2	Local Controller must provide ESD3 Control Actions when Tank Level has reached Low Low. (→STPA-LC.1)
SC-LC.3	Local Controller must provide ESD3 Control Actions when Confirmed Leak Detection. (→STPA-LC.1)
SC-LC.4	Local Controller must provide ESD3 Control Actions when Confirmed Fire or Gas Detection. (→STPA-LC.1)
SC-LC.5	Local Controller must provide ESD3 Control Actions when Confirmed Intrusion Detection. (→STPA-LC.1)
SC-LC.6	Local Controller must provide ESD3 Control Actions when Local Operator has pushed ESD push button in the field. (→STPA-LC.1)
SC-LC.7	Local Controller must provide ESD3 Control Actions when Local Operator has pushed ESD push button in the LCC. (→STPA-LC.1)
SC-LC.8	Local Controller must provide ESD3 Control Actions when Main Controller has provided Local ESD Command. (→STPA-LC.1)

Table 16: Derived Safety Constraints on Local Controller for prevention of UCA-LC.1 “ESD3 actions not provided when required” in a General Station of “Oil Product Pipeline Komsomolsk – De-Kastri”

The same should be performed with the other Unsafe Control Actions identified, so that a comprehensive set of precise safety constraints would be generated.

9.2.3.2 Determining Causes of Identified Unsafe Control Actions

The second step of STPA, once the Unsafe Control Actions have been identified, is to find their potential causes so that ultimately lower-level safety constraints can be defined to prevent them. Table 17 has been generated following the methodology explained in Chapters 4 and 8 of Leveson’s “Engineering a Safer World” [1] and the case study explained in “Safety Assurance in NextGen” [21]. Only causes of the first Unsafe Control Action identified UCA-LC.1 “ESD3 actions not provided when required” have been analyzed for illustration purposes. Ideally, the refined UCAs of Table 16 should be analyzed though.

Figure 9 provides a general control loop and the simplified types of causes (control flaws) to be investigated which might cause Unsafe Control Actions. In this case, as in [21], the arrow between controller and actuator does not include further detail as inappropriate, ineffective and missing control action has been addressed in STPA Step 1 above. Likewise, the arrow between actuator and controlled process on delayed operation is not relevant for UCA-LC.1 “ESD3 actions not provided when required”.

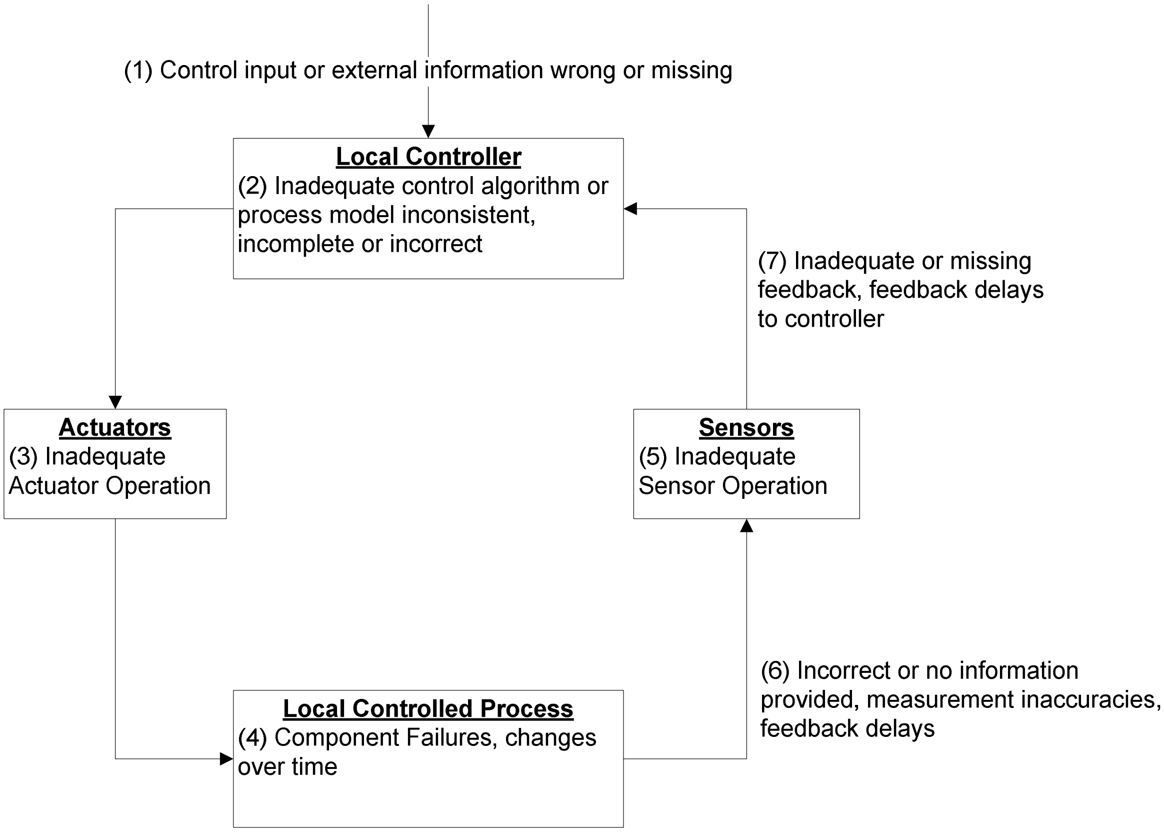

(1) Control input or external information wrong or missing
Local Controller
(2) Inadequate control algorithm or process model inconsistent, incomplete or incorrect
(7) Inadequate or missing feedback, feedback delays to controller
Actuators
(3) Inadequate Actuator Operation
Sensors
(5) Inadequate Sensor Operation
(6) Incorrect or no information provided, measurement inaccuracies, feedback delays
Local Controlled Process
(4) Component Failures, changes over time

Figure 9: General Control Loop for Local Controller with Simplified Types of Causes of Unsafe Control Actions, adapted from [1] and [21]

Table 17 identifies examples of possible causes for UCA-LC.1 "ESD3 actions not provided when required" based on the information of Figure 7.

Hazard H.4 "Fire and/or Explosion" Unsafe Control Action "ESD3 actions not provided when required"	
Process Model Link	**Causes**
(1) Control Input or External Info. Wrong or Missing	-Confirmed Leak Detection not provided by LDS. **Remark:** ESD is usually independent from SCS to avoid common cause failures. The so-called ICSS includes the SCS and the so-called Fail Safe Systems (ESD, F&G, IDS, FFS). LDS is usually part of SCS. -Confirmed F&G Detection not provided by F&G. -Confirmed Intrusion Detection not provided by IDS. -Local ESD command not provided by Local Operator at LCC or field. -Local ESD command not provided by Main Controller.

Hazard H.4 “Fire and/or Explosion” **Unsafe Control Action “ESD3 actions not provided when required”**	
Process Model Link	**Causes**
(2) Inadequate Control Algorithm. Process Model Inconsistent, incomplete or wrong	*Causes of Inadequate Control Algorithm:* -Requirements not passed to designers/ developers or incompletely specified. -Manufacturer’s re-use of standard control algorithms without complete check of adequacy for project specifics. -Control algorithms do not account for feedback loop delays. -Requirements not implemented correctly in software. -Controller components deterioration over time. *Examples of Process Model Incompleteness/ Inconsistencies:* -Simultaneous requests/ commands for Local ESD (e.g. initiated by Local Operator in LCC and by Local Operator in the field) may be provided and the Process Model may not include this scenario. -Controller understanding of tank level signals is wrong. -Controller understanding of Confirmed Detections (LDS, F&G, IDS) is wrong.
(3) Inadequate Actuator Operation	-Communication channel to valves’ actuators becomes corrupted. -Power failure. -Valves’ actuators failures/ degradation over time.
(4) Component Failures/ Changes Over Time	-Valves’ failures/ degradation over time. Pumps failures/ degradation over time (e.g. cavitation). -Failures/ degradation over time of valves’ position monitoring components. -Components’ replacement or environment changes by maintenance operations. -Power failure.
(5) Inadequate Sensor Operation	-Datalink becomes corrupted. -Failures/ degradation over time of tanks’ level transmitters. -Power failure.
(6) Incorrect or No Information Provided, Measurement Inadequacies, Feedback Delays	-Failures/ degradation over time of tanks’ level gauges.

Hazard H.4 "Fire and/or Explosion" Unsafe Control Action "ESD3 actions not provided when required"	
Process Model Link	**Causes**
(7) Inadequate or Missing Feedback to Controller, Feedback Delays	-Feedback on tanks' level not provided. Wrong tanks' level is transmitted. -Power failure.

Table 17: Analysis of Possible Causes leading to "ESD3 actions not provided when required"

These causes can be translated again in lower-level safety constraints to be considered when designing the Local Controller and its components. Some causes of UCAs can be investigated in more detail so that requirements can be generated more precisely and specifically for the project, or the requirement for investigation may be "transferred" (i.e. risk transfer strategy) to component manufacturers.

9.2.4 Discussion

The requirements for the ESD System (which is an element of the Local Controller) captured in the "Operation and Control Philosophy" [18] prepared for the "Oil Product Pipeline Komsomolsk – De-Kastri" are listed as follows:

	System-Level Requirements for the ESD System
LC-ESD.1	*The ESD System shall provide redundancy for all components whose failure would result in loss of control, data or operator interfaces.*
LC-ESD.2	*The Station ESD System shall be connected to Pump Units ESD System to ensure shut down of the pump units in the events of process conditions deviations, process trips or operator initiated ESD (push button).*
LC-ESD.3	*The ESD Systems shall be certified according to IEC 61508 SIL 2 (as a minimum).* **Remark:** SIL Assessment has not been performed in the Project.
LC-ESD.4	*The ESD Systems shall be able to operate in a fail-safe configuration.*
LC-ESD.5	*The ESD Systems shall be designed considering typical failure modes. Common cause failure modes shall be eliminated, where practicable.*

Table 18: ESD System requirements specified in "Operation and Control Philosophy" [18] prepared for the "Oil Product Pipeline Komsomolsk – De-Kastri".

The set of requirements specified in the "Operation and Control Philosophy" [18] is not the result of a hazard analysis. Originally it was planned to perform HAZOP, but as reported above, the project management team (formed by EC and the direct client Design Institute) has decided to exclude this activity due to schedule and budget constraints. Therefore these requirements have been generated following only common industry practice.

The small set of requirements specified in the "Operation and Control Philosophy" [18] seems to put a large emphasis on reliability assurance, while the set of requirements generated using STPA focuses on the identified hazards and their causes. The set of requirements that can be generated with STPA is a lot more comprehensive and precise. While there is no doubt that the quality of the set of requirements obtained with STPA is far better than what it is normally documented in typical Operation and Control Philosophies such as [18], [19] or [20] and the typical specifications of safety-critical systems generated, the desire of generate specifications in such a level of detail so early in the project lifecycle might be arguable, for it seems design organizations do not like to assume too much responsibility during Basic Design and FEED regarding the design to be performed by manufacturers later (regardless of safety-critical or not safety-critical design). On the other hand, the more comprehensive and precise the requirements are, the more accurate prices can be estimated by bidders/ manufacturers and the better the basis on which a contract management/ follow-up can be performed later, therefore overall benefiting the project. This seems to be something to be solved again with a clearly defined Safety Policy.

HAZOP, HAZID and STPA ultimately have in common that they search for causes of deviations of intended behavior to try to manage those (prevent, detect, mitigate). HAZID identifies causes of identified hazardous scenarios, HAZOP identifies causes of process parameters deviations, and STPA identifies causes of hazardous control actions. The type of reasoning involved to arrive to conclusions is rather different from technique to technique (especially because STPA prescribes a systems-theoretic view of causality).

Regarding SIL Assessment, both the objective (i.e. formulate recommendations to achieve a defined target SIL) and the type of reasoning used (i.e. frame provided by IEC 61511) is completely different from STPA. SIL Assessment seems to be rather a risk transfer strategy to the manufacturers at lower levels (i.e. *"The ESD Systems shall be certified according to IEC 61508 SIL 2 as a minimum")*, as opposed to STPA where the reasons why unsafe control actions are executed, are sought. SIL Assessment also seems to be an attempt to create a clear boundary between the responsibility of the systems and sub-systems or components. Instead of trying to find reasons why systems might reach hazardous states in a joint effort, the responsibility and the risk involved is transferred to the manufacturers at lower levels. SIL Assessment does not perform any analysis of causes. It is observed that SIL should be rather interpreted as a quality standard to be delivered by manufacturers (i.e. it is rather about fulfilling a reliability target), not as a safety standard.

Besides the findings discussed above, a practical advantage of STPA is that it can be performed independently by an analyst or by a team of analysts. It does not need a formal panel of experts (as for HAZID or HAZOP), which normally requires extra resources for an organization. Issues such as rank in the organization and dominant personalities typically bias the documentation of results of the exercise (even if the exercise has been contracted to a third party).

While it seems that performing STPA to a satisfactory level of completion can be very lengthy, HAZID, HAZOP and SIL Assessment are not short exercises to perform and it is also difficult to achieve a satisfactory level of completion.

10 Documenting System Limitations

In a similar way as for Environmental Assumptions, the list of input data part of the Basis of Design [14] included some limitations. Also the studies performed during concept selection (i) Pipeline System Selection Study [11], (ii) Oil Product Logistic Transportation Model Study [12] and (iii) Multiproduct Technology Study aiming to ensure Product Quality [13]. The table below shows some examples.

	Some Limitations for Project Example	**Type**
L1.	*Pipeline Maximum Allowable Operating Pressure is 91.88 barg. (→Pipeline System Selection Study [11], ↑2.4)*	*Trade-off*
L2.	*Minimum Acceptable Operating Pressure is 2 barg. (→Pipeline System Selection Study [11])*	*Functional*
L3.	*Pipeline Minimum Batch Size for oil products is 20,000 m^3. (→Oil Product Transportation Study [12], ↑C.24)*	*Trade-off*
L4.	*Pipeline Maximum Allowable Boost Rate is 2%. (→Oil Product Transportation Study [12], ↑2.4)*	*Trade-off*
L5.	*Maximum Allowable Wind Speed for Tanker Loading Operations is 10 m/s.*	*Uncontrolled Hazard*
L6.	*Maximum Allowable Wave Height for Tanker Loading Operations is 2 m.*	*Uncontrolled Hazard*
L7.	*Multiple berths at the loading point in Port De-Kastri cannot load the same oil product at a time. (→Oil Product Transportation Study [12])*	*Functional*
L8.	*A single tanker at the loading point in Port De-Kastri cannot load multiple oil products at a time. (→Oil Product Transportation Study [12])*	*Functional*
L9.	*Berth 1 Minimum Capacity is 0 DWT and Maximum Capacity is 40,000 DWT. (→Oil Product Transportation Study [12])*	*Functional*
L10.	*Berth 2 Minimum Capacity is 40,000 DWT and Maximum Capacity is 100,000 DWT. (→Oil Product Transportation Study [12])*	*Functional*

Table 19: Examples of Limitations identified for the Komsomolsk – De-Kastri Project [11], [12], [14]

11 Considering relevant Operations Experience in the Design Development

In this Project Example, EC's direct client Design Institute and its client as well as investor and most likely future operator of the pipeline system have provided poor input regarding available experience. Most of the time, they have referred to Russian norms and standards and have instructed EC to gather information from that literature. Russian norms and standards are, however, more prescriptive than illustrative of the experience which has triggered establishing them. Since the intent of Design Institute with this contract was to try to find better solutions to be compared with the solutions of the previous Investment Justification, their general strategy has been one way learning from EC rather than sharing. This might have also been influenced by schedule constraints, which have again played a decisive role (as in many other projects) not allowing for open discussions on lessons learned for example.

The high-level operations constraints listed in the tables above have been identified by analysis of available experience mainly related to (i) general pipeline systems operations, (ii) port operations and (iii) specific multiproduct transport operations. This available experience has been elicited from experts in EC and from the body of knowledge of the Oil & Gas industry.

12 Delivering Safety Requirements and Constraints to Operations

The sections above provide examples of the type of information to be produced and how to connect the different bits with pointers. The following tables provide references to the tables in the main thesis document.

Safety Information	**Reference to Examples provided in Tables above**
Operational Assumptions	Some in Table 6 and Table 7
Safety Constraints	- Safety Constraints in Table 4 - High-level Operation Constraints in Table 9 - Lower Level Operation Requirements and Design Constraints in Table 11
Safety-related Design Features	Table 12
Operating Assumptions	Some in Table 6 and Table 7
Safety-related Operational Limitations	Table 19

Table 20: References to Examples of Safety Information (to be passed to Operations) for the Komsomolsk – De-Kastri Project

Examples for (i) training and operating instructions, (ii) operational procedures, (iii) audits and performance assessment requirements as well as (iv) safety verification and analysis results have not been developed for the Project Example because these are not part of the scope of work for the current project phase.

Appendix 3 Example of Integrating Safety into Architecture Selection and System Trade Studies

(not included)