NTNU

Norwegian University of
Science and Technology

Systems-Theoretic Process Analysis (STPA) Applied to the Operation of Fully Autonomous Vessels

Jiahui Zou

Reliability, Availability, Maintainability and Safety (RAMS)
Submission date: July 2018
Supervisor: Mary Ann Lundteigen, MTP
Co-supervisor: HyungJu Kim, MTP
Jon Arne Glomsrud, DNV-GL

Norwegian University of Science and Technology
Department of Mechanical and Industrial Engineering

NTNU

Faculty of Engineering
Department of Mechanical and Industrial Engineering

Date
2018-06-28

MASTER'S THESIS SPRING 2018
FOR
STUD.TECHN. Jiahui Zou

Systems-Theoretic Process Analysis (STPA) applied to the operation of fully autonomous vessels

[Norwegian Working Title]

The main objective of this master thesis is bringing new insights and suggestions for the practical application and benefits of STPA, using the analysis of the operation of a fully autonomous vessel as a case study. The main contribution is a list of suggested improvements to the STPA concerning the framing, focusing, and prioritization within each analysis step. The focus will be on the application of STPA in the early design phase where main functions, but not the detailed realization, have been decided.

To meet this objective, the following tasks are to be carried out:

1. Introduce briefly motivation and the main steps and terminologies of STPA, and present and discuss the challenges in applying the STPA as identified in in the specialization project. Challenges should include those identified in literature survey and those identified in the analysis a concept for a fully autonomously operated vessel.
2. Introduce two other methods that may apply to hazards identification: control HAZOP, which is directed to analysis of control systems, and functional FMECA, which is commonly used as a top-down/high level analysis. Carry out both analysis using the operation of the autonomous vessel as case study, compare the results and application in light of findings in task 1.
3. Identify and discuss specific improvements to STPA, based on task 1 and task 2.
4. Carry out an STPA analysis using the improved method, then discuss the results in light of the identified challenges in task 1.
5. Suggest ideas for further research.

Contact:
Supervisor 1: Mary Ann Lundteigen (NTNU), Jon Arne Glomsrud (DNV-GL)
Supervisor 2: HyungJu Kim (NTNU)

Address:
NO-7491 TRONDHEIM
Norway

Org.nr. +47 93970668
Email: jiahuiz@stud.ntnu.no
mtp-info@mtp.ntnu.no
https://www.ntnu.edu/mtp

RAMS

Reliability, Availability, Maintainability, and Safety

Systems-Theoretic Process Analysis (STPA) Applied to the Operation of Fully Autonomous Vessels

Jiahui Zou

August 2018

MASTER THESIS

Department of Mechanical and Industrial Engineering
Norwegian University of Science and Technology

Supervisor 1: Mary Ann Lundteigen (NTNU), Jon Arne Glomsrud (DNV-GL)

Supervisor 2: HyungJu Kim (NTNU)

.

Preface

This report documents my master thesis written during the spring of 2018. The thesis has been carried out in the 2-year master program of RAMS (Reliability, Availability, Maintainability and Safety), at the Norwegian University of Science and Technology.

This thesis has been written with the guidance of my supervisor professor Mary Ann Lundteigen and co-supervisor HyungJu Kim at the department of mechanical and industrial engineering. Supervisor Jon Arne Glomsrud, who from DNV-GL, also provided much important feedback and industrial practices of autonomous vessel.

The reader of this thesis is assumed to have some basic knowledge in RAMS, risk analysis and should be familiar with basic concept of marine operation.

Trondheim, 2017-01-22

Jiahui, Zou

Acknowledgment

Firstly, I would like to thank my supervisor, Mary Ann Lundteigen for her sincere help and continuous guidance for this project. Even with a tight schedule, she is always able to arrange a weekly meeting with me to share my progress and solve problems. Further thanks to my co-supervisor HyungJu Kim, it always inspired me a lot from discussion with him. I am really grateful for his friendly attitude and harsh comments. My thanks also go to Jon Arne Glomsrud, who makes constructive suggestions on the establishment of concept of autnomous vessel.

Here I am given a chance to express my appreciation to all my friends in Trondheim, it is their company that support me to go through 2 year's period in Trondheim. I will never forget all the best time with RAMS group. Special thanks go to my parents XiangYi and Ping, I would not be where I am today without your unselfish love.

Jiahui Zou

Executive Summary

Fully autonomous vehicles are still in the early stages of development but showing great potential benefits. ReVolt is an electrically propelled, autonomous concept container model ship designed by DNV GL to minimize the energy consumption and cost. However, lacking knowledge and operational experience with fully autonomous systems, risk hidden in autonomous operation need to be identified. The main objective of this thesis is to bring new insights and suggestions for the practical application and benefits of Systems Theoretic Process Analysis (STPA), using the analysis of the operation of a fully autonomous vessel as a case study

This thesis mainly carries out three tasks. The first task is enhancing STPA concept by concluding challenges found in specialization report and literature study for a fully autonomously operated vessel. Then traditional risk analysis methods FMECA and HAZOP, especially functional FMECA and control HAZOP are introduced to seek for an opportunity to improve original STPA method based on their attributes. Based on the results achieved from previous tasks, in task 3, an improved STPA method of certain step is established and implemented. Problems and challenges left before are discussed.

For the purpose of achieving comparable results and avoiding complex analysis, all risk identification methods are carried out for autonomous vessel Guidance control system at a high level.

Contents

Chapter 1

Introduction

1.1 Background and motivation

For centuries people are continuously pursuing an easier life, especially the process speeds up for last years. In the form of quadrotor helicopter, under water robot, robotic vacuum cleaner and smart house, remote control and artificial intelligence are gradually creeps into daily lives by the advantages of technology. Taking advantages of these inventions, to be more specific, unmanned operating system is capable to emancipate people from the dangerous or repeated work. However, challenged by worker displacement and Large initial investment[1, 2], the potential risk of automation is also put forward to be solved.

ReVolt is an electrically propelled, autonomous concept container ship designed by DNV-GL to minimize the energy consumption and cost. Travelled from Trondheim to Oslo, the project is focus on minimizing cost of crew and fuel to achieve short distance transport of goods.

Accoding to Kongsberg's concept of fully autonomous vessel, YARA Birkeland, a fully autonomously operated vessel is assumed to be unman-operated and environmental friendly. Fully autonomous ships have potential to reduce human-based errors, but at the same time may modify some existing risks as well as create new types of risk. These circumstances and possible remedies need to be explored.

To achieve the purpose of establishing safe design requirements and verification objectives, a continuous hazard identification approach such as Systems-Theoretic Process Analysis (STPA) is suggested at design phase.

STPA, as a new developed hazard identification approach, it is interesting to see STPA implementation into autonomous vessel safe operation. Based on the results from specialization report, this master thesis will firstly conclude the challenges identified before. Then functional FMEA (FFMEA) and control HAZOP (CHAZOP) is introduced and carried out to seek for alternative solutions for safety-related problems. Thus, according to the findings, an improved STPA approach which take advantages of both functional FMEA and control HAZOP will be put forward. It is also interesting to compare and further discuss modified STPA results and challenges with original STPA approach.

In March 2018, Nancy *et al* [3] published the second version of STPA Handbook, which bring new requirements and guidance to STPA implementation.

1.2 Problem description

Since the concept of fully autonomous vessel is still in developing phase, the hazards and problems hidden in autonomous operation can not be avoided. Generally, collision and grounding, technical problems (i.e. technical maintenance), cyber-attacks, autonomy assisted accidents (i.e. radar assisted accident) have become the main threats to the autonomous vessel.

For a semi fully/fully autonomous vessel, based on the experience from specialization report, it is acceptable to set a high-level analysis boundary to avoid extensive analysis. To be more specific, in hazard identification method STPA, obstacles can be reflected at the definition of control action and process model. The more detailed process model is established, the more complex unsafe control actions

are identified. The complexity is mainly reflected in the number and definition of unsafe control actions.

Furthermore, original STPA approach is capable to identify unsafe control actions and provide corresponding safety constraints. However, these results are still waiting to be compared with other risk identification methods such as FMEA and HAZOP. Moreover, the limitations and challenges left in specialization report remain to be solved. The importance of controllers, the hidden hazardous unsafe control action and general structure of analysis are still waiting to be discussed.

1.3 Project scope

1.3.1 Objectives

The main objective of this report is to carry out a case study about the STPA to discuss opportunities and challenges of performing STPA for autonomous ships. It is also interesting to identify methods to improve original STPA based on the attributes by comparing STPA with functional FMEA and control HAZOP. To realize these objectives, the following tasks have been performed:

1. Clarify conceptions in relation to autonomy and strategies for autonomous operation.

2. Introduce autonomous operation system concept of a vessel, based on but not limited to Revolt.

3. Establish a control loop diagram based on fully-autonomous vessel.

4. Introduce and compare two approaches for implementing STPA, demonstrate the application using a simple case study.

5. Carry out STPA analysis and identify unsafe control actions, figure out casual factors and safety constrains based on a specific control action. (Above tasks have been completed in specialization report)

6. Conclude the advantages and drawbacks during original STPA implementation. Identify approaches to improve original STPA by solving existed problems, in the light of comparison between STPA with other methods.

7. Introduce FMEA and HAZOP to give an overview of traditional risk identification methods. Focus specifically on FFMEA and CHAZOP.

8. Implement a full FFMEA and CHAZOP approaches for Guidance controller of autonomous vessel operation, summarize the advantages and limitations of each method. Try to identify the opportunities to improve original STPA based on the findings in FFMEA and CHAZOP implementation process.

9. Carry out a case study of the improved STPA approach on certain steps, make a comparison between the original STPA application.

10. Discuss key results and re-conclude advantages and challenges of improved STPA method. Put forward recommendations and plans for the further research.

1.3.2 Research approach

Literature reviews on FMECA and HAZOP has been performed to learn about the basic knowledge and applications. NTNU course TPK5160 Risk Analysis contributed much efforts on the review of these two risk analysis methods.

Furthermore, the technical problem is identified based on the professional supervisions and some ideas and suggestions are from the industrial companies: DNV-GL. After discussing with experienced experts Tor Onshus and Jon Arne with autonomous vessel and safe operation, desired method and research scope of the thesis is finally chosen.

1.3.3 Limitations

Because of the time limit and lacking practical experience about autonomous operation, this thesis has the following limitations:

1. The control loop diagram has been established at high-level. It needs to be further discussed defining the control system into Environmental Awareness, Guidance system and Motion controller. All sensors and controllers are assumed with no redundancy which are over optimistic.

2. The thesis defines a high-level control actions and process models to avoid extensive results. In reality, autonomous vessel operation and the environmental factors should be more complex, which presents detailed requirements for the definition of control actions and process models.

3. An Unsafe Control Action (UCA) is a control action that, in a particular context and worst-case environment, will lead to a hazard[3]. After acquiring the theoretic foundation, an attempt to develop a qualitative and quantitative model need to be done. This will contribute much effort on identifying priority of UCAs and vital safety constraints. However, since autonomous vessel is still in developing phase, this thesis is basically established on a qualitative method without quantitative data from events.

4. No matter STPA, FFMEA or CHAZOP, these risk identification methods are established as a brainstorming approach and carried out by a experienced

group. Limited by time and personal experience, this thesis can not avoid mistakes during implementation process.

1.4 Thesis structure

The rest of the report are organized as follows:

Chapter 2: Give overview of autonomous operation system. Definitions and classifications related to autonomous vessel are documented here. This chapter will also introduce the industry states and standard framework in autonomy field. Most content in this chapter is adapted from specialization report.

Chapter 3: Introduce briefly motivation and the main steps of STPA, and present and discuss the challenges in applying the STPA as identified in in the specialization project. Challenges include those identified in literature survey and those identified in the analysis a concept for a fully autonomously operated vessel. Most content in Chapter 3 is adapted from specialization report.

Chapter 4: Introduce risk identification theories of FMEA and HAZOP, additional attention is paid to functional FMEA and control HAZOP.

Chapter 5: Introduce and conduct full analysis of functional FMEA and control HAZOP step by step in the light of fully autonomous vessel. Document corresponding results and conclude the difficulties identified during the process. Propose and discuss opportunities to improve original STPA, based on the findings of FFMEA, CHAZOP.

Chapter 6: Carry out a modified STPA analysis for certain step using the improved method, discuss the results compared with challenges identified in specialization project.

Chapter 7: Conclude and discuss results and findings from the previous chapters. The research respective is also proposed for future development in autonomous operation.

Chapter 2

Autonomous Vessel Operation

2.1 Background

Since computer technologies increasingly developed in recent years, computer-based systems have significantly influenced shipping industry. It also put forward new requirements to the autonomous vessel operations. Computer based systems, generally referred to as Programmable Electronic Systems (PESs)[4], are being used to perform safety-related functions. With the basic components of sensor, controllers and actuators, autonomous vessel control system can be considered as a combination of individual Programmable Electronic Systems. According to IEC 61511, plant safety is achieved by a number of protective systems and relies on many technologies: mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic systems. Any safety strategy must therefore consider not only all the elements within the individual programmable electronic system (e.g. sensors, logic solvers. actuators) but also all the safety related systems making up the safety of the plant[4].

Defined by ROSS Gemini Centre, safety-critical systems are systems introduced to prevent, or mitigate the consequences of hazardous events. Since autonomous operations are implemented by electrical, electronic, and/or programmable electronic technologies, with interaction to mechanical systems and systems for communication and human interface. Hence, to prevent and mitigate the consequences of hazardous events, it is necessary to view autonomous control system as a safety-critical system and carry out corresponding risk identification methods.

2.2 Definition and Developments

ABS[5] is a company which delivers great classification services, technology leadership, and trusted technical advice for marine and offshore industries. Accoding to ABS, autonomous vessel is defined as “Marine vessel with sensors, automated navigation, propulsion and auxiliary systems, with the decision logic to follow mission plans, sense the environment, adjust mission execution for the environment, and operate without human intervention”[6].

Advances in autonomy which have been a research area for more than one century are driving the development of maritime industry. The first automation of ships date back to 1911, when the American entrepreneur Elmer Sperry’s gyrocompass invention made it possible to get a reliable measurement of the ships’ heading[7]. Based on the measured heading from the gyroscope, an automatic pilot could steer the heading of the ship without constant human intervention[8]. Developed by Balchen *et al*[9], the first DP-system based on Linear-Quadratic-Gaussia controllers was proved to have significant impact on ship operations. Further, many new projects on autonomous maritime transport are initiated currently accompanied by collaborations between companies and universities. Projects such as NOVIMAR project (TU Delft with European Commission’s Horizon2020, 2017), ReVolt project (NTNU with DNV-GL, 2013) and ROBOAT project (TU Delft, MIT, with AMS Institute) developed a lot, researches focus more on automation of marine vessel with reduced human interaction[10].

2.3 Industry and Research Status

2.3.1 Overall industry status for autonomous vessel

Governments around the world are looking for an acceptable way to move more cargo to sea in order to contain the spiraling costs of road maintenance caused by heavy lorry

traffic, not to mention labor cost and air pollution[11]. Norway is a country which benefits significantly from shipping (fourth largest fleet in the world) and offshore industries[12]. Consequently, it also put forward a higher transportation requirement on vessels. Autonomy, as one of the solution, is seen as a possibility for maritime transport to meet today's and tomorrow's competitiveness, safety and sustainability challenges. Norway has taken the lead in exploring innovative ways of tackling this issue by bridging more fjords and sea passages to ease transit process. In 2016 government agencies and industry bodies established the Norwegian Forum for Autonomous Ships (NFAS) to promote the concept of unmanned shipping[13]. In support of these efforts, the Norwegian government has turned the Trondheim Fjord into a test-bed for autonomous ship trials. Other nations such as Finland (AAWA project) and China (CCS project in Zhuhai), are pursuing similar goals.

Playing a role as research leaders in Norway, Rolls-Royce, Kongsberg Maritime and are currently exploring and developing vessels to be autonomous.

Stella was designed by Rolls-Royce. As a ferries passenger vessel operated on protected waters of the Archipelago Sea between Korpo and Houtskär will have additional sensors for testing purpose[14].

YARA Birkeland which designed by Kongsberg Maritime, is the World's first autonomous cargo vessel, planned to sail in the Norwegian fjords, and is scheduled for fully autonomous operation in 2020[15].

Finished in 2015, Maritime Unmanned Navigation through Intelligence in Networks Project (MUNIN project), aimed to verify the safety and feasibility of how far can all the functions of a ship be automated. Within MUNIN's idea of an autonomous and unmanned vessel both generic alternatives will be combined in a holistic concept. Developing and validating a suitable mixture of remote and automated technology for ships will be the core task of the MUNIN project[16].

2.3.2 A brief introduction to ReVolt

The increasing stress placed on land based logistic networks is driving the search for alternatives. Therefore, researchers at international certification body and classification society DNV GL have developed “ReVolt”, a concept vessel that designed to be an environmentally friendly solution, suitable for short sea shipping along the coast of Norway[17]. Autonomous, fully battery powered and highly efficient, “ReVolt” is a new shipping concept that offers a possible solution to the growing need for safety, intelligence and transport capacity.

During spring 2015, NTNU student Eivind Finne Riley[18] who from department of Marine Technology designed an optimized wave foil system aiming to minimize the required battery capacity on the ReVolt ship.

In June 2017, two students Henrik Alfheim and Kjetil Muggerud[19], who from department of Engineering Cybernetics, NTNU carried out a study of the dynamic positioning system of 1:20 ReVolt model. The main objective of their thesis was to develop a DP control system to achieve accurate and precise low-speed navigation. The control system, sensor fusion and collision avoidance of the model ship ReVolt has been immensely improved, simulated, implemented and tested with experimental sea trials.

Figure 2.1: The concept ship ReVolt (DNV GL)

At present, ReVolt model is capable to follow a desired trajectory under help from navigational sensors. The preliminary calculations show that the needed power output for sailing at 6 knots in calm seas is merely 50kW. However, equipment and functions such as robot operating system simulator, waypoint tracking, path following, environmental sensors and collision avoidance are still waiting to be further developed[20].

2.4 **Regulatory Framing**

The International Maritime Organization (IMO) is the global regulator for shipping, intends to test the safety and security of autonomous surface ships to ensure they are environmentally sound and not hazardous to other maritime users[21]. IMO continuously attempts to ensure the safety of maritime operations[22] by providing international conventions such as the International Convention for the Safety of Life at Sea (SOLAS) and particular safety management guidelines such as the International Management Code for the Safe Operation of Ships and Pollution prevention (ISM Code).

In May 2018, the IMO has officially commenced work to look into how safe, secure and environmentally sound Maritime Autonomous Surface Ships (MASS) operations may be addressed in IMO instruments.

However, the biggest problem in autonomous vessel industry is that, autonomous vessels haven't been specifically addressed by a systematic international rule or regulation so far[23]. In this respect, lacking of legal framework for autonomous ships will be further exposed.

2.5 Classification

Thomas Sheridan presented levels of autonomy (LOA) in 1978. Sheridan defined vary continuous range of levels, from the lowest level of fully manual performance to the highest level of fully autonomous without any inputs from human[24, 25]. Based on work from Sheridan, NHTSA, SAE international standard and Lloyd's Register have developed different LOA scales. However, a common conclusion is that, such LOA sales may not be applicable to all operation modes when applied to different subtasks of autonomous machine[26].

Lloyd's Register, a leading international provider of classification, compliance and consultancy services to the marine industry[27], has set out a guidance to provide the route to classification with six levels for autonomous ships.

The autonomy level system devotes to make clarity to designers, shipbuilders, equipment manufacturers, ship owners and operators, and enabling accurate specification of the desired level of autonomy in design and operations.

Table 2.1: Autonomy Levels adapted from Lloyd's Register

Autonomy Level	Autonomy Level Description	Decision	Actions	Exceptions	System capability(driving modes)
Human operator monitors the driving environment		Manual	Manual	Manual	N/A
AL 0: Manual steering	The operator is on board or performs remote control via radio link.				
AL 1: Decision-support on board	The operator monitors and changes the course and speed, if necessary.	Human in the loop with on board data	Manual	Manual	Some driving modes
AL 2: On-board or shore-based decision support	Operator monitors operation and surroundings, changes course and speed if necessary. Proposals for interventions are given by system.	Human in the loop with on/off board data	Manual	Manual	Some driving modes
Automated operating system ("system") monitors the driving environment		Human supervision (Ship level)	Human supervision (Ship level)	Human supervision (Ship level)	Some driving modes
AL 3: Execution with human being who monitors and approves	Operator monitors the system's function and approves actions before they are executed.				
AL 4: Execution with human being who monitors and can intervene	Operator monitors the system's functioning and intervenes if considered necessary. Monitoring can be shore-based.	Human supervision (Broad level)	Human supervision (Broad level)	Human supervision (Broad level)	Some driving modes
AL 5: Monitored autonomy	After a destination is determined by operator, the system executes the actions calculated by itself. The operator is contacted if necessary.	Rarely supervised	Rarely supervised	Rarely supervised	**Most driving modes**
AL 6: Full autonomy	System makes independent decisions for all situations without human involved.	Unsupervised	Unsupervised	Unsupervised	**All driving modes**

It can be concluded that, from AL 0 to 2, vessels still need to be operated by human operators. Information can be provided on shore to make decisions. An AL 3 ship will enable operator involved for system monitoring and actions making. Human could intercede and control autonomous operations. An AL 4 ship is advanced than AL 3, human, as a supervisor, only need to intervene if necessary. Shore-based monitoring is applicable from this stage. As a half-autonomous ship, AL 5 still required human intervenes when uncertain situations happened. AL6 ships are considered fully autonomous, where decisions are calculated by the system and being performed.

Clients will need to decide which level of autonomy they want to operate at, as these are complex projects. Ships do not have to be fully autonomous, but the AL needs to be decided at the design stage. The autonomy level is not necessary constant, it can be flexible changing according to practical situation.

2.6 Autonomy in Different Modes of Operation

For autonomous ship, vessel behavior and human intervention will be dependent on predetermined tasks and states of vessels. Under complex environment, a “flexible” or “dynamic” autonomy is therefore necessary to be implemented. The concept “Dynamic Autonomy”[26] is defined to enable vessels jump from different autonomy levels to make responses according to the practical situations. In some cases, for instance, when ships operating on open seas, a nearly fully autonomous can be achieved. Human operator can also be contacted and intervene to provide supervision and decisions unless system is very certain about its surroundings and calculated actions. Variable autonomy levels are accessible if unexpected catastrophic disaster such as tornado occurred. In further development of autonomous vessel, the ships will be asked to perform this type of “Dynamic Autonomy” approach depending on the missions and actual environments.

Ships may loss of communication with shore accidently due to human error. In this

case, a degressive autonomy level is applied from “shore-based monitoring and execution” to “manual operating” mode. An example is shown in figure 1 to demonstrate when fully autonomous ship lost their function. Fully autonomy is no longer maintained and will degrade to lower level accordingly.

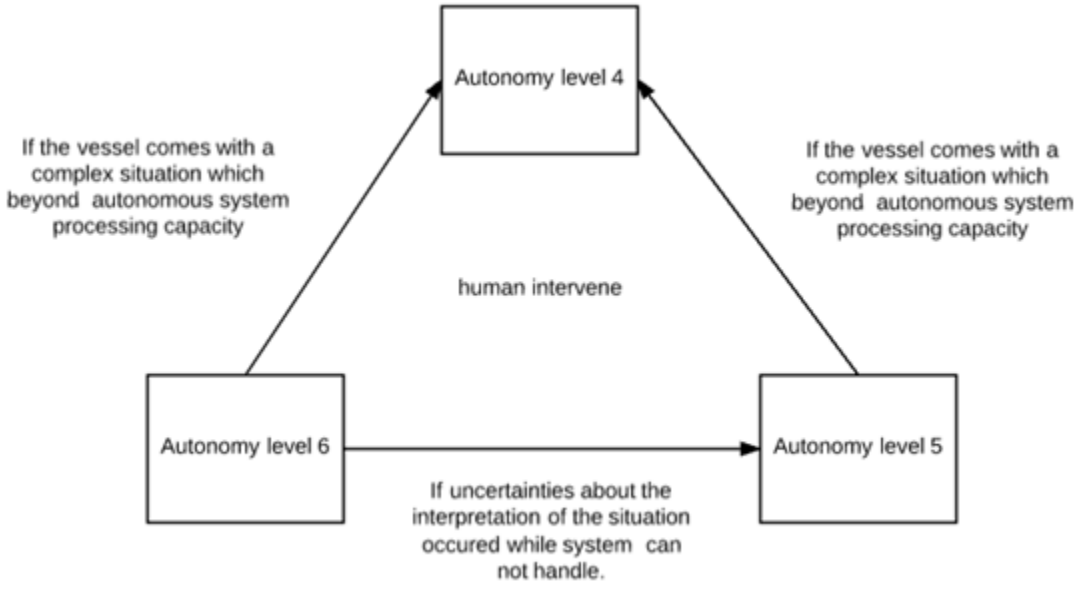


Figure 2.2: “Dynamic Autonomy” degradation.

Due to time and experience limit, except of chapter 2.1 and 2.3.2, most content are cited from specialization report.

Chapter 3

STPA Methodology

3.1 STPA Introduction

STPA[3] is a relatively new hazard analysis technique based on an extended model of accident causation. System-Theoretic Accident Model and Processes (STAMP)[3] is the name of the new accident causality model based on systems theory, which provides the theoretical foundation for STPA. In system design and development phase, by considering risk management as a control function, STPA enables STAMP ideas for a practical implementation[28]. Basically, STPA has the same goals with other hazard identification methods, that is, to identify hazardous scenarios and then try to provide safety constrains to reduce failure frequencies and mitigate consequences of unwanted events[28].

Since STPA works on the hierarchical safety control structure, it can be used both on technical design and on organizational design. More importantly, it can be used at any phase of design process[28]. For instance, using early in system development process to figure out high-level safety constraints and requirements enables a lower cost at starting phase. This claim is because, by designing work flow early to avoid further rework, the cost of applying STPA at the beginning phase is negligible. This step can also be used to perform a Preliminary Hazard Analysis[28]. However, the structure of STPA can be complicated during developing process by defining various process models. A further optimize work such as merging process models for unsafe control actions identification can be carried out to avoid an over-complex design.

STPA is a top-down method, as Fault tree analysis. However, the typical difference is that, STPA uses a model of the system that consists of a functional control diagram instead of a physical component diagram used by traditional hazard analysis methods. STPA is based on system theory unlike FMEA, which is based on reliability theory. Moreover, STPA considers safety as a system's control (constraint) problem rather than a component failure problem[29].

In contrast to the traditional hazard analysis techniques, STPA can be more precise in aspect of identifying safety requirements since these constrains are identified from each causal factor and hazardous scenario, particularly those related to software, system design, and human behavior[28].

3.2 Main steps of STPA

STPA was firstly introduced in "Engineering a Safer World" by Nancy G. Leveson. The author then wrote a STPA primer to supplement the book for STPA implementation.

In "An STPA primer" version 1 august 2013[28], the author had defined three steps to summarize STPA procedures, that is:

0. Describe and establish the foundation of system.

1. Identifying unsafe control actions.

2. Identifying the causes of the unsafe control actions.

STPA Handbook[3] provided a new framework of STPA procedures which can be more systematic and scientific:

1. Define the purpose of the analysis.

2. Model the control structure.

3. Identify unsafe control actions.

4. Identify loss scenarios.

The first step defines the scope and system boundary of analysis. It will also determine specific level of research goal by setting desired application area. For instance, STPA method can be applied from a basic goal “Preventing loss of human life” to a broad concept such as “Ensuring system security, privacy and performance”.

In the second step, a control structure that captures system functions and interactions is established as a set of feedback control loop. The control loop diagram may draw from a high-level structure to a detail-level structure according to the depth of analysis.

Unsafe control actions are identified in the third step to reflect how they could lead to the losses defined in the first step. Furthermore, identified UCAs will also be used to create functional requirements and constraints for the system in the next step.

The final step identifies the reasons why unsafe control might occur in the system. UCA scenarios and corresponding reasons and mitigation measures are suggested in this phase.

Limited by time, the author chooses not to perform the new STPA method in this thesis. Thus, the further work is still based on the original STPA method introduced in STPA primer.

Detailed STPA procedures have been introduced and implemented through a case study in specialization report, which is assumed as the basics of understanding this master thesis. Furthermore, for the purpose of achieving a scientific result, challenges and problems leaving in specialization report are necessary to be solved in thesis.

3.3 Problems conclusion

Based on chapter 6.2 in specialization report, left problems can be concluded as follows:

1. Dynamic autonomy. Autonomous vessel may need human intervention when facing a complex environment. In a catastrophic situation, for example, an autonomous vessel which at level 6 may degrade to level 5 or even lower level to maintain its basic function. It brings a problem that, should we consider human factors for a fully autonomous vessel and if so, how can we carry out STPA approach with a dynamic autonomy.

2. STPA level definition. Precise process models which list in series will geometrically increase the work load. One of the difficulties applying STPA is to define a proper level of process models. Moreover, STPA introduced four default “guide words” for UCAs identification table in step 1. Those default “guide words” can be further discussed and developed

3. “Fake safe”. A safe status under high level STPA implementation may ignore further unsafe actions of the autonomous operation.

4. Controllers interacting failures. Inspired from Asim Abdulkhaleq and Stefan Wagner[30], STPA may has difficulties to provide an action table and casual factors for multiple controllers with interference among the actions. It happens on a system level controller which has sub-controllers in the control loop of a system.

In this master thesis, the author will identify an improved STPA approach based on functional FMEA and control HAZOP. Thus, new results can be compared to check if previous problems are solved.

Chapter 3.1 and most context in chapter 3.2 are adapted from specialization report. This chapter initially intended to introduce the new STPA method described in STPA Handbook, the intention is eventually abandoned due to time limitation.

Chapter 4

Risk Identification Method

Though original STPA in specialization report roughly identified high-level unsafe control actions for one control action with one process model of Guidance controller, the remaining limitations and challenges alert original STPA is not a fully developed hazard identification method. For this reason, another risk identification method need to be implemented to provide conferences even opportunities to improve original STPA.

This chapter will briefly present two traditional risk identification methods “FMEA and HAZOP” and its branch method “FFMEA and CHAZOP”. The main purpose of this chapter is to conduct literature studies for a basic understanding of traditional risk identification methods.

Especially, this chapter will introduce three implementation approaches of CHAZOP. Based on author’s understanding, the overall process of CHAZOP is same with HAZOP, the only difference is guidewords and parameters.

4.1 FMEA

Developed in the late 1940s to identify problems in military systems, FMEA is analysis method that is used to identify potential failure modes with the causes for all the parts in system to find negative effects[31]. Traditional FMEA is carried out for each component in a technical system to identify and describe the possible failure modes, failure causes, and failure effects[32]. The main task of FMEA is to identify potential

problems in the early design phase or product that can affect its safety and performance, identify measures to mitigate or minimize the effects of the identified potential problems (failure modes).

Compared to a top-down analysis method, FMEA can augment or complement Fault Tree Analysis (FTA) and identify many more causes and failure modes resulting in top-level symptoms as a bottom-up analysis method[33]. Therefore, failures in a lower level will become corresponding failure modes at the next level until the overall system.

Failure modes and effects criticality analysis (FMECA) is an extension to FMEA which describe or rank the severity of various failure modes.

There is no official definition of categories of FMEA method at present. Generally, FMEA can be divided into software FMEA, hardware FMEA and interface FMEA. Functional FMEA, as a branch of software FMEA, is interesting to identify its application and possibilities in improving original STPA method.

4.2 Functional FMEA

Functional FMEA is a tool that allows a team to systematically identify, document, and prioritize potential functional failure modes, their effects and causes[34]. This analysis may be performed at the functional level until the design has matured sufficiently to identify specific hardware that will perform the functions.

Functional FMEA, as a family member of FMEA, like its ally design FMEA and process FMEA, relies on the team experience to identify the level or criticality of potential problems. The difference between functional FMEA and its relatives is that, the mean purpose of functional FMEA is not determine mitigation measures but identify and avoid possible accidents at design phase. More precisely, FFMEA aims to identify and

analyze potential issues thereby identifying new system functionality or design ideas that can be incorporated into the yet to be designed system[34]. Performed as a pro-active tool, the system will also become more robust and failure resilient, benefit from the functionality and features that identified.

4.3 **HAZOP**

HAZOP study is a systematic hazard identification process that is carried out by a group of experts (a HAZOP team) to explore how the system or a plant may deviate from the design intent and create hazards and operability problems[32]. Developed from chemical industry[35], HAZOP has been adapted to other industrial areas such as computer, which is known as CHAZOP.

The HAZOP analysis is performed in brainstorming meetings which supported by guidewords, process parameters, and various checklists. Firstly, the system or plant is divided into a number of study nodes that examined in sequence. Then guidewords and process parameters are used in brainstorming sessions to give rise to proposals for possible deviations in the system[32]. Based on the deviations identified above, possible causes and consequences are determined for related mitigation measures. Finally, a structured HAZOP report sheet is completed for the further research field.

During the design phase of a new or upgraded process plant, process risk assessment is routinely performed, using widely accepted techniques such as HAZOP[36, 37]. However, the inadequacy of HAZOP became apparent when the failure of one of the computers controlling a polymerization reaction failed, resulting in a total uncontrolled plant shutdown, and loss of containment[38]. The increased use and growing sophistication of computer-based systems to control process facilities has led to an awareness of the value of addressing computer systems within the HAZOP framework[39]. Therefore, to achieve the purpose of reducing control system risks, a

number of valuable modifications of the HAZOP technique have been proposed such as process HAZOP, human HAZOP, procedure HAZOP and software HAZOP[32].

In general, although the proposed procedures seek to overcome the difficulties of applying the HAZOP technique to programmable electronic systems, consistent application of a standardized procedure for CHAZOP is yet to be achieved[38, 39].

This thesis will try to introduce and carry out a brief CHAZOP approach for the autonomous control system, especially for Guidance controller.

4.4 Control HAZOP

4.4.1 Introduction

As mentioned earlier, because of the successful application of HAZOP and widespread use of computers in the process industry, researchers and engineers are suggesting ways of adapting HAZOP to safety-critical systems[40]. However, HAZOP study did not address the root explanations of deviations, some of which are attributable to malfunction or failure of programmable electronic systems[38]. Therefore, a specific HAZOP need to be established to analyze computer-based systems.

The term CHAZOP (Control systems HAZOP, or Computer HAZOP) has been applied to several types of study, which differ in their objectives and methodology[41].

CHAZOP is most commonly[41] considered as Control systems HAZOP when Performing a workshop study to assess the risks and impact of a control system failure on the process, using a What-If/Checklist style approach.

It is also acceptable to view CHAZOP as Computer HAZOP when Performing software criticality analysis in the control system.

As an extension of HAZOP, the purpose of CHAZOP is to find possible causes of process upset due to control system failure[41].

CHAZOP is also highly useful for sequence control systems involving reactive chemical hazards, normally unmanned operations where high reliability and online time is required, and where complex interlocks and their sequence is critical for safety[38].

4.4.2 Possible Approaches

A useful summary of some different approaches for CHZOP implantation is provided by Kletz[42] in his book *Computer Control and Human Error*. This section will briefly introduce three approaches mentioned by Kletz.

Approach 1 Guide words and parameters combinations

Since CHAZOP can be viewed as the extension of conventional HAZOP, one obvious approach to perform CHAZOP is to simply replace or supplement the process-related guide words and deviations with computer-related ones. Identified by Burns and Pitblado[43], there are mainly two types of guide words for reviewing computer control systems. One set is for considering the hardware and logic of the system, and the other is for considering human factors.

Except from the conventional guide words “No, More, Less, Wrong” applied by Burns and Pitblado, the draft guideline for CHAZOP produced by the UK Ministry of Defense[44] extends the list of guide words associated with conventional HAZOP with the following words: early, late, before and after. Similar to the guidewords used in STPA method, the word *early* and *late* are relevant to the time of process actions while *before* and *after* are relevant to the actions sequence.

Moreover, Cameron[38] has devised a set of application-specific guide words and deviations which focused on the PES. Parameters are divided into four categories:

a) Digital hardware (Modules, cards, cables, connectors, switches, monitors, keyboards, network equipment.)

b) Software (program, memory)

c) Communications (data signals)

d) Mechanical items (mainly origin and destination items in the control loop e.g. sensors and actuators).

A piping and instrumentation diagram (P&ID) shows the piping and related components of a physical process flow. Cameron suggested that, CHAZOP could ignore the mechanical items integral to the P&ID since it can be covered in the conventional HAZOP. In this paper, the author will briefly implement CHAZOP based on this method, detailed procedures can be found at next section.

Parameters can be collected by considering all the links between different components on the control loop diagram, such as data (signal) flow, control flow, data rate, data value, event, action, repetition time, response time and encoding. Thus, the possible deviations can be defined as the combination of CHAZOP guide words with control process parameters. It also should be noticed that, not all combinations are meaningful. Only appropriate and relevant deviations (parameter with guide word) are chosen for CHAZOP analysis.

Approach 2 Preliminary and full CHZOP

Generally, it is recognized that CHAZOP should be carried out separately from HAZOP[37, 41]. However, Andow's approach[37] indicates that CHAZOP can be integrated into conventional HAZOP or at least coordinate these two approaches closely.

Andow[37] suggested that CHAZOP should be done in two stages: preliminary and full.

They are really different studies at different stages in the development of a project.

Carried out as part of early HAZOP, the purpose of a preliminary CHAZOP is to identify early in design critical factors that influence the overall architecture and functionality of the system. Preliminary CHAZOP mainly consider three aspects at the early stage: the proposed architecture of system, safety-related functions, system-level hazards and failures. It also states that, preliminary CHAZOP should not divorce from preliminary plant HAZOP, instead, it is highly recommended to be integrated if possible.

The full CHAZOP is a further work of preliminary CHAZOP after coding is complete. Research goal is to evaluate the design in detail at a later stage and confirm the findings in preliminary CHAZOP. The team should consider three different aspects of the system after system design complete essentially:

a) computer system/environment

b) input/output (I/O) signals

c) complex control schemes

The questions relating to the computer system/environment are essentially larger scale, these issues are normally considered at early design phase rather than detailed, process-related test that CHAZOP applied.

Input/output signals issues can be usefully combined with the deviations suggested by Bums and Pitblado, according to the report by Kletz[42]. Moreover, questions relating to I/O signals (what should happen? will the operator know? What should operator do? does it matter? propagation? changes needed?) are similar to those applied within the conventional HAZOP framework and should always be raised for each guideword + parameter combination. These questions still follow HAZOP framework and not structurally different to the guideword + parameter combinations.

For complex control schemes, the schemes are used to establish the basis of process procedures. In each scheme the operator need to consider its functions and mode of operation.

Preliminary/full CHZOP approach usefully restricts the scope of matters to detailed hazard identification allowing a sense of P&ID finalization proportion and focus to be established[39].

Approach 3 Control types

Lear[45] contributed much effort on the distinction in the types of control undertaken by PES through suggesting independent consideration of continuous control and sequence control. Each of these considerations identify short- and long-term power supply failure with dedicated checklists and separate study sessions. Though the separations are a desired approach of maintaining focus, however, it can also be resource intensive and time consuming.

The distinctions made by Lear are consistent with the approach suggested by Nimmo *et al* [46] that takes into account software interactions and the effect on the process. Nimmo and his colleagues recognized that, the assessment procedure is geared towards understanding how the computer will respond to a process deviation and how the computer will control and affect the process. Based on conventional HAZOP in the process industry, the full CHAZOP scheme as outlined cannot be applied in the early stages of the design process to identify any potential problems.

Chapter 5

Risk Identification Method Application

This chapter will briefly implement FFMEA and CHAZOP approaches to compare and seek for an opportunity to improve original STPA. In order to make a reasonable comparison, research target and analysis level need to be unified at the same level. Hence, this section will choose a unique system of autonomous vessel, guidance system, on which a high-level analysis is applied.

5.1 Functional FMEA implementation

Accoding to the original FMEA method described by Marvin Rausand[32] and functional FMEA introduced by Stuart Burge[34], the main steps of functional FMEA can be concluded as follows.

System Breakdown and Functional Analyses (Functional FMEA step 1)

In this step, a function block diagram is established to determine interrelationships between the various subsystems. Component functions and their performance requirements for each component should be identified. It is also important to describe the operational and environmental stresses that may affect the system and its operation.

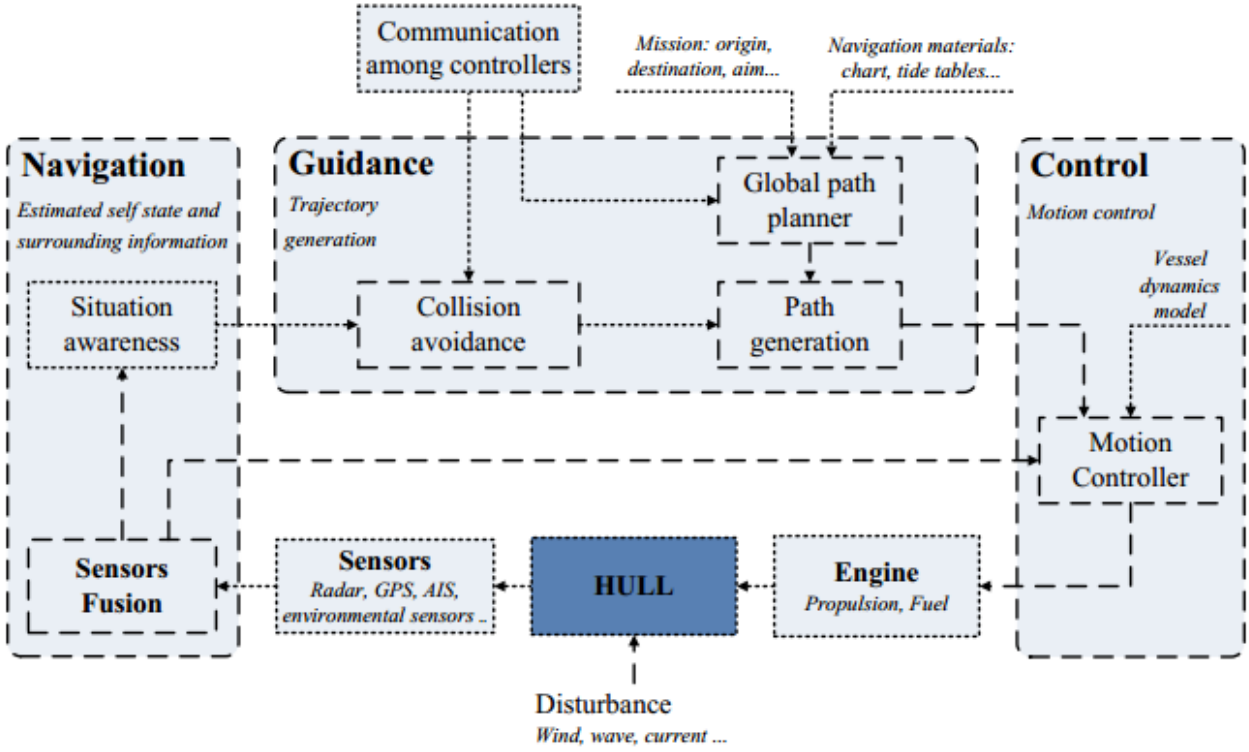


Figure 5.1: Function diagram for an autonomous vessel (adapted from Matteo Schiaretti.etc.)

Based on high-level analysis of fully autonomous vessel, the main function of Guidance system can be concluded as:

1. Calculate and generate feasible path.

2. Re-route when required or in emergency.

3. Collision Avoidance.

Identify the potential failure modes and causes (step 2)

For each component, the relevant failure modes and failure causes are identified in this phase.

To achieve the purpose of describing the unusual actions, a simple way is to use "Anti-functions" verbs such as "Over, Under, No, Intermittent, Unintentional or unintended." For instance, one of the possible failure modes of function "Calculate and generate feasible path" can be:

1. No calculation.
2. Incorrect calculation.
3. Over detailed calculation
4. Over simple calculation
5. Intermittent calculation

The possible causes for the first failure mode "No calculation" can be:

1. Guidance control components fails to perform its function.
2. Not enough corresponding information provided from actuator, weather forecast and situation awareness, thus guidance control refuse to perform calculations.
3. Human remote operator takes control when emergencies situations.

Identify the current detection method employed (step 3)

Failure detection based on the assumption that the system has a designed or similar model before which may has experienced the failure mode. Thus, detection or prevention methods which incorporated in the previous design may provide help and references to the mitigation measures

Determine the Consequences (step 4).

For each failure mode, the credible consequences need to be identified and documented. The effects can be sub-system level and system level. Subsystem level indicates relevant functions failed while the system level may stop the whole production/operation.

In relevant to the autonomous system, the possible consequences can be ranked such as “tolerable”, “maintenance work required”, “system break down” according to the severity.

Risk Assessment (step 5)

In this step, the frequency and severity of the consequences of each failure mode are estimated and recorded in classes. Evaluation standards vary from failure rate, severity, detectability and RPN. Since this report does not involve quantitative calculations, this step can be discussed and developed in future work provided by enough data.

Design suggestions (step 6)

Risk-reducing measures, responsible and comments are listed in this phase. Possible actions to correct the failure and restore the function or prevent serious consequences are then recorded.

Based on above steps, a typical functional FMEA worksheet (one function in Guidance system) can be established as table 5.1. The steps above are repeated for all functions in autonomous vessel control system until a full FFMEA approach complete.

Table 5.1: An example of FFMEA worksheet for autonomous vessel Guidance system

FFMEA worksheet: Guidance control						
Function	**Potential functional failure mode**	**Potential functional failure cause**	**Potential functional failure effect**	**Detection of failures**	**Frequency/Severity/RPN**	**Mitigation measures**
Calculate and generate feasible path	No calculations Incorrect calculations Over detailed calculations Over simple calculations Intermittent calculations	Guidance control components fails to perform its function Not enough information provided to support calculations Emergencies situations	SHIP fail to calculate and generate new path, ship will stop and maintenance work is required.	Periodic function self -tests		

The function of Guidance system is identified from function block diagram in advance, then potential functional failure mode is identified by combine “Anti-functions” verbs with functions. Corresponding causes and consequences are provided at a high level. Frequency/Severity/RPN and Mitigation measures columns are empty due to lack of data and information.

5.2 Functional FMEA conclusion

Compared with original STPA method, this section will try to identify an improving proposal based on the experience of FMEA implementation.

5.2.1 Limitations

Exclusion of human frailties and errors. It is a common phenomenon that, human errors result in miss operations that do not cause equipment failures are often not considered. However, human factors should not be ignored especially at the design phase. In the aspect of fully autonomous vessel, though it is assumed no operators on board, there still exists potential possibility of human errors in maintenance work or remote operations.

Only one level of cause and effect at a time. Since failure modes and process models are analyzed once a time, multiple and interactive combinations of failure modes and causes can be overlooked. Moreover, the level of cause and effect is also limited at a time.

Dependency on the mode of operation. The effect of failure mode relies on the system operation, while the unsafe control actions depending on the process model. Those interactive relationships significantly limit the verities of potential effects.

5.2.2 Opportunities

It can be noticed that, when describing failure modes, functional FMEA uses “Anti-functions” verbs such as “Over, Under, No, Intermittent, Unintentional or unintended”. Compared to original STPA, it puts forward criteria which beyond normal STPA’s unsafe

control action descriptions: Intermittent and unintentional. With more specific definition criteria on unsafe control actions, the accuracy and frame of unsafe control actions will be significantly guaranteed.

It can be noticed that, FFMEA is similar with STPA in some extent. For instance, FFMEA intends to break system into functional subsystems. Then, a functional block diagram can be established accordingly. However, STPA consider whole system as a control system with controllers, a control loop diagram is then established. For the autonomous operating system described in specialization report, control loop diagram is established and further developed based on the function block diagram. It indicates an opportunity that, with a proper level/structure of function block diagram, FFMEA could provide potential help on establishment of control loop diagram in STPA.

5.3 CHAZOP implementation

In this section, the author will try to perform a CHAZOP study based on approach 1 proposed by Burns *et al* and Cameron. Based on literature reviews, overall process of CHAZOP is same with HAZOP, the only difference is CHAZOP has guidewords and parameters

Step 1: Plan and Prepare

Firstly, before the first HAZOP meeting, the required information should be provided for control system such as process flowsheet and control system logic diagram.

In specialization report, a control loop diagram is established to provide information process of a fully autonomous vessel. The autonomous operating system is divided into four components for analysis, which are physical vessel, sensors, controllers and actuator respectively. To compare the results with FFMEA, the CHAZOP approach is

necessary to keep the same level (high-level) in analyzing process. Thus, a specified control loop diagram for Guidance controller is established to provide information flow as figure 5.1.

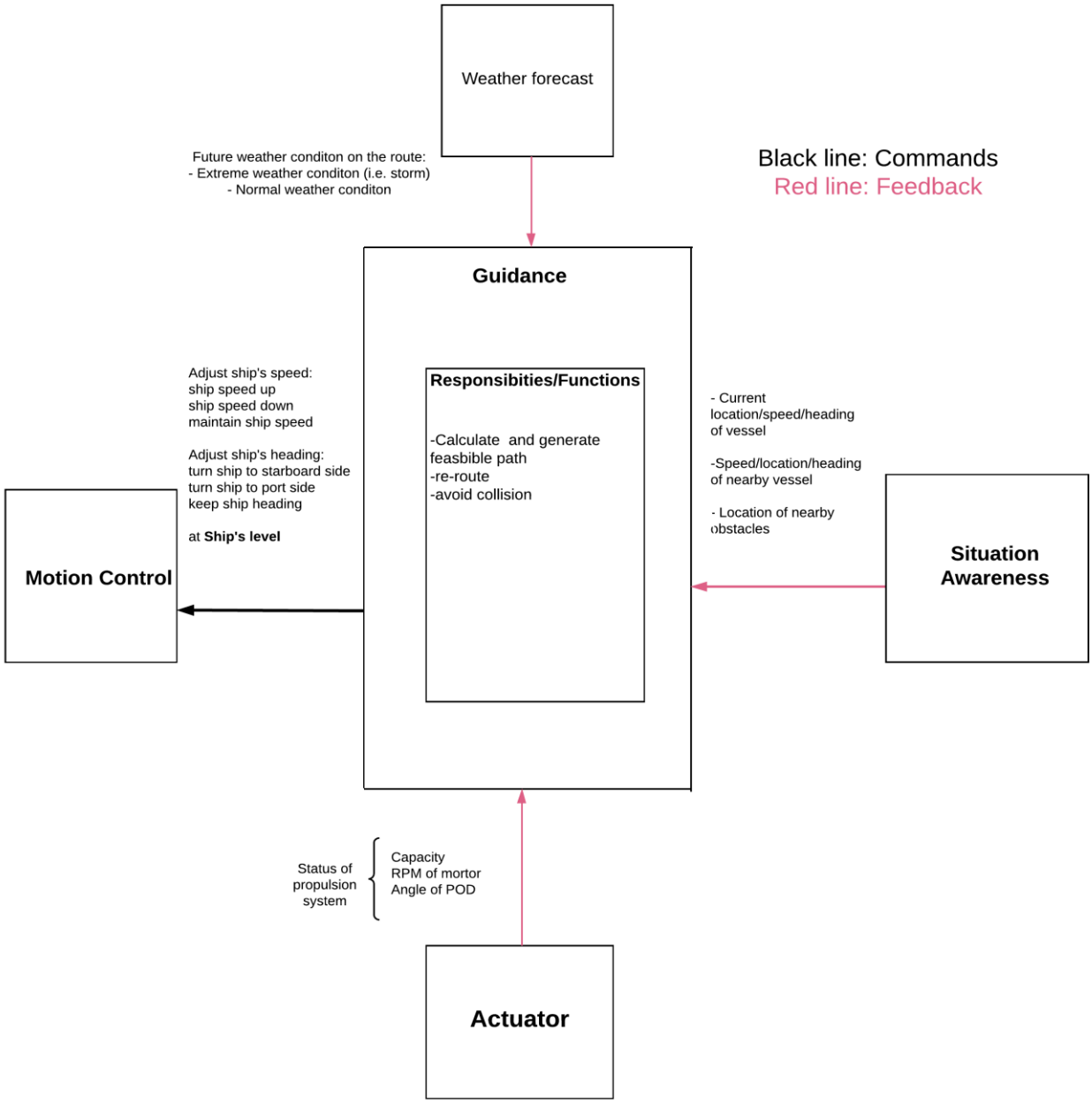


Figure 5.1: Control system logic diagram for Guidance controller (Adapted from control loop diagram)

Step 2: Identify Possible Deviations

This step will firstly examine the normal state of process parameters, after choosing a study note, combinations of CHAZOP guide words and process parameters are determined to guide the team into identifying process deviations and the causes of the deviations.

Step 3: Identify Deviation Causes and Consequence

To identify the possible causes of a deviation is an important part of the HAZOP study.

Corresponding causes and consequences of deviations can be found at table 5.2.

Step 4: Identify Safeguards and Propose improvements

To be able to come up with relevant proposals for improvement, the HAZOP team must be familiar with the existing barriers (safeguards) that have already been incorporated in the system. Furthermore, Possible actions to prevent the deviation or to mitigate the consequences are recorded.

Since CHAZOP carried out at design phase, in which not enough information is provided. The column of barriers and improvements will be filled after more information is provided.

The steps above are repeated for all nodes, deviations, causes and consequences identified until full CHAZOP complete.

According to Cameron's suggestion, one example CHAZOP table for Guidance controller can be established as table 5.2. Despite of traditional information flow with study notes, interacting factors such as digital hardware, software and mechanical items are used

to set a scope of CHAZOP analysis.

Table 5.2: An example of CHAZOP worksheet for autonomous vessel Guidance system

CAHZOP Worksheet: Guidance controller								
	study note	parameter	guideword	deviation	possible causes	possible consequences	barriers	proposed improvements
communication	Data flow from Guidance controller to Motion Controller	signal/data flow	no	zero data transmission	no data input from evironmental detector, sensor fustion and actuator	Guidance system break down, ship stop working	self-monitoring system, etc.	
			part of	incomplete data	insufficient/missing data input from evironmental detector, sensor fustion and actuator	Guidance system function failed, ship stop working		
			more	redundant data/repeated data	not relevant/repeated data input from evironmental detector, sensor fustion and actuator	Guidance system cost more unnecessary time , working effiency reduced		
			other than	excessive noise/corrupt signal	undesired data input from evironmental detector, sensor fustion and actuator	Guidance system function failed, ship stop working		
			early/late	signal generated too early/late	inappropriate input from evironmental detector or sensor fustion; inappropriate response from actuator	Guidance system make wrong decision, ship need maintenance work		
			before/after	Incorrect signal sequence	inappropriate data transmission speed	Guidance system function failed, ship stop working		
digital hardware		card	no	I/O failure	quality of control card	Guidance system break down, ship stop working		
			more	multiple failure	conflict between card and processor			
			part of	partial failure of card	quality of control card			
software		program	no	program corruption	programmer error			
		memory	more	memory overflow	memory error			
mechanical items	Data flow from Envoronment	environment sensor	part of	insufficient data	insufficient/missing data input from environment			
	Data flow from Actuator to Guidance controller	actuator	no	zero data transmission	no data input from Motion controller, or actuator fail to send report to Guidance controller			
			part of	incomplete data	insufficient/missing data input from Motion controller, or actuator fail to send full report to Guidance controller			

5.4 CHAZOP conclusion

Ideas on how CHAZOP should be done are still evolving. Thus, the drawbacks and advantages of a CHAZOP approach is highly dependent on the procedure descriptions. Based on the scheme applied above, the result of CHAZOP method can be concluded as follows.

5.4.1 Obstacles

Boundary setting. This also happened in STPA approach in which, the system or element boundaries are set to focus on intend target, especially on failure initiation and mechanism. For instance, both CHAZOP and STPA method set a high-level boundary for the fully autonomous operating system to pursue a preliminary result for further analyzing. Sometimes apparently arbitrary boundaries must be set to maintain manageable element size. More specifically, the process system selection (loop-by-loop, nodes, etc.) is restricted by the system size and control components must be unified by an identifiable design intention.

Time is another obstacle. As mentioned by Andow[37], after the preliminary CHAZOP is complete, the CHAZOP approach should be the opportunity for detailed, focused examination of full CHAZOP. However, full CAHZOP will put a higher requirement on the team size and experience with an increasingly detailed analyzing process. STPA comes with similar problems of the analyzing depth, the consumed time and system complexity is also increased by performing a detailed level analyzing.

5.4.2 Advantages

Systematic guide word framework can be a common advantage for CHAZOP and STPA.

As described in CHAZOP approach, not all guide words are meaningful and useful. Similarly, STPA normally used four types of control command states, but analysts can add/remove any states depending on the analyzed system.

More importantly, CHAZOP provides a more systematic way to define parameters. Except from traditional study notes, interactive subsystems such as software/ hardware, human factors, communications, environmental conditions and actuator are considered as aspects of deviations during CHAZOP analyzing process, which gives an interesting proposal to re-define the scope of scenarios used in STPA approach.

Chapter 6

A modified STPA approach

Based on the experience from conducting FFMEA and CHAZOP approaches, this report mainly proposed 2 possible approaches to improve original STPA method. Limited by the time and experience, the modified STPA approach in this chapter is established on the STPA primer version 1 published in 2013.

6.1 Potential improvement 1

It can be noticed from FFMEA and CHAZOP that, appropriate guide words play an important role in defining hazardous events. Concluded from FFMEA and CHAZOP, possible guide words include “No, Over (More), Under (Part of), Intermittent, Early/Late, Before/After, Unintentional or unintended (other than)”. Compared with four types of control command states used in STPA, guide words from FFMEA and CHAZOP may re-define and enlarge the scope of UCAs.

The modification could reflect on the STPA step 4, if we take table 5.6 as an example.

Table 6.1: A brief example of UCAs identification for guidance system (Adapted from

specialization report 2017 autumn)

Control action	Process model	UCAs			
ship speed up	Collision avoidance	Not provided causes hazard	Provided causes hazard	Provided too early/too late causes hazard	Stopped too soon/Apply too long causes hazard
	Can not avoid collision	[UCA-1]	[UCA-2]	[UCA-3]	[UCA-4]
	Avoid collision by speed up	[UCA-5] Speed up command is not provided when speed up is needed to avoid collision		Late: [UCA-6] Speed up is executed too late cause collision	Soon: [UCA-7] Ship ends accelerating halfway and certain speed is not achieved to avoid collision Long: [UCA-8] Ship keeps accelerating after it reaches desired speed cause collision
	Avoid collision by speed down		[UCA-9] Ship inappropriately speed up when a reduced speed is required	N/A	N/A
	Avoid collision by a maintained speed		[UCA-10] Ship inappropriately speed up when a constant speed is required	N/A	N/A

If we take guide word “Intermittent, Unintentional or unintended (other than)” into consideration, a new-guideword table of Guidance system UCAs can be shown as table 6.2.

Table 6.2: A brief example of UCAs identification for guidance system with new guide words

Control action	Process model	UCAs					
	Collision avoidance	Not provided causes hazard	Provided causes hazard	Provided too early/too late causes hazard	Stopped too soon/Apply too long causes hazard	Provide Intermittently cause hazard	Provide unintendedly causes hazard
ship speed up	Can not avoid collision	[UCA-1]	[UCA-2]	[UCA-3]	[UCA-4]	[UCA-5]	[UCA-6] Human intervention when ship in emergent situation (Dynamic Autonomy)
	Avoid collision by speed up	[UCA-7] Speed up command is not provided when speed up is needed to avoid collision		Late: [UCA-8] Speed up is executed too late cause collision	Soon: [UCA-9] Ship ends accelerating halfway and certain speed is not achieved to avoid collision	[UCA-11] Desired speed is not achieved because speed up command is provided intermittently	[UCA-12] Irrelevant command, data validation problem, hardware problems

					Long: [UCA-10] Ship keeps acceleratin g after it reaches desired speed cause collision		
	Avoid collision by speed down		[UCA-13] Ship inappropri ately speed up when a reduced speed is required	N/A	N/A	N/A	
	Avoid collision by a maintain ed speed		[UCA-14] Ship inappropri ately speed up when a constant speed is required	N/A	N/A	N/A	

Compared with original STPA method, modified UCAs identification approach found another 4 UCAs which original STPA easily ignored.

For UCA-6, human factors are considered when ship comes with emergent accidents in which a shore-based remote control is required and performed. In this case, human errors in operation should not be ignored since it always cited as a primary cause contributing factor in disasters and accidents[47]. Normally, human factors are not considered in fully autonomous operation. Assumed that, original STPA could carry out

an enough detail-level analysis in which human factors are considered for emergent response, the UCAs identification table will be rather complex and time-consuming. Therefore, the modified STPA approach has shown its advantages at the system design phase with a high-level analysis.

UCA-11 considers a situation that a speed accelerating command is given but intermittently. Therefore, vessel fails to reach the desired speed in the end and the collision still happens. It seems that, UCA-11 is easily confused with UCA-9 with a similar UCA description. The difference focus on the continuity of control actions. Control action in UCA-11 is a repeated activity with a possible scenario “Information input with incorrect sequence”, while control action in UCA-9 is assumed to provide shortly. Similar with the case in UCA-6, guide word “Provided too soon cause hazard” will eventually identify same UCAs with guide word “Provided intermittently cause hazard” in low-level analysis. However, the process could be time-consuming.

UCA-12 describes a situation in which control action is provided but irrelevant. For instance, when an accelerating speed is required for collision avoidance, corresponding speed up command is provided along with irrelevant commands such as “adjusting ship heading” and hardware/software problems.

STPA primer introduced a general table for identifying UCAs, which contains four control command states in step 1. Default control command states are “Not providing causes hazard, Providing causes hazard, Too early/too late, wrong order causes hazard and Stopping too soon/applying too long causes hazard”. But it seems there is not a standard for control command states. Hence, the advancement of modified STPA method can be reflected at the flexibility of control command states for a certain unsafe control action. By defining desired control command states at a proper level, certain level UCAs are easier to be reached. For instance, when fully autonomous vessel operating in certain environment in which emergent response happens frequently and cannot be ignored, shore-based human intervene is then required. Both original STPA

and modified STPA can identify human factors UCAs in the end, but original STPA with default control command states will cost more time and efforts compared to modified STPA method, which is able to identify human factors UCA directly at high level.

Generally, identified UCAs are highly dependent on the level of process modes. A high-level process mode will guarantee a rather high-level UCAs, which are significantly helpful at the design phase. However, with the process modes described more detailly, the scope of UCAs will be enlarged which lead to a complex result. Moreover, it also can be noticed that, not all guide words are meaningful in the UCAs identification process. This suggest the importance of a flexible UCAs identification table which contains desired-level process model and proper guide words.

6.2 Potential improvement 2

Guide words plus parameters used in CHAZOP provide a solution to describe possible deviations. Cameron suggested a systematic way to summarize the framework of deviations. Inspired by Cameron, when conducting original STPA step 5&6 to identify casual factors and safety constrains for a specific UCA, scenarios can also list systematically with key words “Communication, Hardware, Software and Mechanical items”. Therefore, instead of determining scenarios by group brainstorming, a rigorous framework of scenarios can be established to avoid missing points and repeated work. The following table is designed for UCA-5 in table 6.1, only one scenario is considered due to length and time limit.

Table 6.3: Scenarios, causal factors and safety constraints for UCA-5

[UCA-5] Speed up command is not provided when speed up Is needed to avoid collision			
ID	Scenario	casual factors	safety constrains
	Communications		
S-1	Guidance system does not receive information input from Situation awareness	S-1-CF-1) Situation awareness controller fail to send current vessel status to Guidance controller.	S-1-SC-1) Information about current status of vessel (i.e. ship speed) must always be sent from situation system
	Digital Hardware		
S-2	Guidance system experienced a I/O cards breakdown	S-2-CF-1) Control card blown a fuse	S-2-SC-1) Control card must always be functional and transit data to Guidance controller.
S-3	Guidance system experienced a component interacting process (control card, processor rack, processor)	S-3-CF-1) Intensive communication in/with Guidance controllers	S-3-SC-1) Interacting intensity must stay at a reasonable level
	Software		
S-4	Guidance system experienced a data failure	S-4-CF-1) Guidance system make programable errors	S-4-SC-1) Guidance system need to carry out period self-check
	Mechanical items		
S-5	Guidance system does not receive information input from weather forecast	S-5-CF-1) Weather forecast fail to send current vessel status to Guidance controller. etc.	S-5-SC-1) Information about current status of environment must always be sent from weather forecast

S-6	Guidance system does not receive feedback from Actuator	S-6-CF-1) Actuator fail to send current vessel status to Guidance controller. etc.	S-6-SC-1) Information about current status of propulsion system (i.e. motor RPM) must always be sent from weather forecast

Adaptive Cruise Control (ACC) is an automotive feature that allows a vehicle's cruise control system to adapt the vehicle's speed to the traffic environment. ACC system has two controller modules: ACC module and Engine Control Module (ECM), which are connected together and used to control the vehicle speed. Both of them receive the vehicle speed information from the brake control module. ECM sends brake switch command to the ACC module and the ACC module sends the ACC state target speed to ECM. Described by Asim Abdulkhaleq[30], STPA has limitations for analyzing interacting controllers in the control loop of a system. It can be reflected that hazards occur without component failures[48].

Similar to the ACC system, Guidance controller generally has two sub-controllers based on its function: calculation controller and path generation controller. They both receive data from environmental sensors, situation awareness and feedback from actuator. Calculation controller send path changing command to path generation controller, while path generation controller send re-calculation command to calculation controller. Thus, it can be assumed that, STPA has limitations of analyzing interacting controllers in the autonomous control system. Assumed a hazardous case in which Guidance controller performs its designed function accompanied with unnecessary intensive interaction between calculation controller and path generation controller. Scenario 6 in table 6.3 identified this situation with the modified STPA approach.

In original STPA method, scenarios are identified by group brainstorming. The process of scenarios identification is based on analysts experience and capacity. However, for an individual analyst who implement the whole STPA step 2, it is unavoidable to omit

scenarios and corresponding casual factors. Table 6.3 established a systematic analyzing framework for scenarios that covers “Communication, Digital Hardware, Software and Mechanical items” to be used in identifying casual factors. Thus, without missing key factors such as “Operator, Hardware/software and Interacting systems”, the causes for UCAs will be identified more scientifically to cover most possible fields of control system.

6.3 Conclusion

As mentioned in the STPA handbook published at March 2018, the STPA system theory is never a fully developed concept and it is still in developing process. Traditional hazard analysis methods, such as fault tree analysis (FTA), failure modes and effects criticality analysis (FMECA), event tree analysis (ETA), and hazard and operability analysis (HAZOP) exits potential possibilities to improve original STPA method. FFMEA and CHAZOP, which focus on components functions and control process respectively, could provide a new horizon in both method theory and detailed procedures.

Limited by time and experience, this chapter only focus on the Guidance controller in the control system. Furthermore, in order to compare methods results, FFMEA, CHAZOP and modified STPA method are all restricted at high-level. With a further investigation which steps into a low-level research, the complexity would promote a desired STPA approach with an appropriate level in autonomous operation field.

Chapter 7

Summary

7.1 Summary and Conclusions

The objective of this master thesis is to assess the feasibility of using the STPA for hazard identification and assessment of complex and fully autonomous operating systems. As a continuous work from autumn 2017, this article also assessed the possibility of using an improved STPA method for hazard identification of the autonomous vessel control system based on a case study and comparison with the FFMEA and CHAZOP. Since fully autonomous vessel is still in designed phase without any international regulations and standards, the corresponding risk analysis approaches are still incomplete and required further development.

This report firstly provides an overview of autonomous operation in the fields of autonomous vessel. Industry states and standard framework in autonomy field are introduced to provide a basic research background. Then the motivation and the main steps of STPA are presented. The challenges left in specialization report are specifically discussed to seek for favorable solutions in the rest of the paper. For that reason, traditional hazard identification method FMEA and HAZOP, especially functional FMEA and control HAZOP for Guidance controller are conducted and documented. Specific limitations and opportunities in improving original STPA are identified and discussed particularly. Finally, an improved STPA implementation on fully autonomous vessel is carried out. During this process, additional unsafe control actions hidden in information communications are identified with control process guide words. It is also

interesting to establish a scientific framework considering “Communication, Hardware/Software and Mechanical items” to scope the unsafe control actions scenarios. In this case, corresponding casual factors and mitigation measures can be systematically provided for each unsafe control action.

The main result of this thesis is, by conducting FFMEA and CHAZOP approaches, two potential applications are identified which may improve original STPA method. The first application area is that, though STPA has default control command states which is “Providing causes hazard, Not providing causes hazard, Applied too long/Stopped too soon causes hazard and wrong timing/order causes hazard”, the level and content of the control command states is not unchangeable. Thus, by defining goal-oriented control command state at a desired level, certain UCAs can be identified with less time and efforts. Another result of this thesis is that, a scientific structure of scenarios identification framework is established. Since scenarios, casual factors and safety constraints are identified by an experienced group brainstorming in STPA step 2, it is unavoidable to omit certain cases. The situation goes even worse for an individual person due to time and experience limit. However, if we take advantages of FFMEA and CHAZOP by setting a scientific framework of scenarios categories, such as “Communication, human factor, digital hardware/software and mechanic items”, it can be a more systematic approach to STPA implementation by analyzing individual and interactive component failure.

In conclusion, the proposed STPA approach, as a complementary activity to the original STPA method, seems to be feasible and beneficial because the it covers goal-oriented hazards with a scientific framework that are hardly covered by the original STPA approach. Further explanations can be found in discussions in this chapter.

7.2 Discussion

To begin with, it is interesting to discuss the autonomy level for a fully autonomous vessel. DNV-GL designed ReVolt as a "unmanned, zero-emission, shortsea vessel", which is assumed as a fully autonomous vessel at AL 6 according to table 2.1. However, described by DNV-GL[49] and previous research[19], "fully" autonomous vessel may not be the best choice in the near future. The difference between fully autonomous and semi-autonomous focuses on the human factor. If autonomous vessel needs the operator/monitor on shore who may intervene autonomous operation, then it seems better to be a semi-autonomous. Moreover, compared with computers, human beings may be more flexible and sophisticated when faced with complex situations such as cyber-attack and disaster. Thus, a highly automated vessel with few crew on board can be a wise idea for the next step.

This article outlines a methodology aimed at improving the current verification and testing approach for maritime systems such as control system by introducing a specialized STPA for identifying verification objectives. This has been done to address four challenges in specialization report:

1. Dynamic autonomy.

2. STPA level definition.

3. "Fake safe".

4. Controllers interacting failures.

For the first challenge, since the level of autonomous vessel is not invariable, fully autonomous vessel may degrade into semi-autonomous vessel or even manual steering in emergent situations. In that case, human factors can not be ignored in hazard identification process. UCA-6 in Table 5.2 successfully identified this case with less

efforts than original STPA at high-level. It also indicates that, the "UCA guide words" may significantly influence UCAs. A goal-oriented control command state may save much time than default control command state. Thus, how to define a proper guide words could be a key factor when identifying UCAs.

Solutions for challenge 2 and 3 are similar, that is, to set a desired level for STPA analyzing. If we take table 5.1 as an example, the system is assumed to be safe when speed up action is provided for collision avoidance. However, the safe state will degrade to an unsafe state when control action provided incorrectly. Furthermore, since process models are merged in both cases, UCA cases are significantly reduced. In other word, precise process models which list in series will geometrically increase the work load. Above two cases both indicate the importance of a proper STPA analyzing level. Generally, a high-level STPA method can be performed in early concept analysis to assist in identifying safety requirements and constraints. With the analyzing process moves to a lower level, the whole STPA process could be more complex and time-consuming.

Challenge 4 indicates the importance of scenario structure. Table 6.3 provided a scientific way to define scenarios in which "communication, hardware/software (human factor) and interacting items" are considered. Thus, rather than brainstorming, a scientific structure will ensure hazard analysis include most potential causal factors in losses.

In current stage, the modified STPA approach successfully identified additional UCAs with less effort than original STPA. Moreover, almost all the challenges left in specialization report have been analyzed in the thesis. Therefore, the advancement of the improved STPA are obvious and significant.

Generally, this thesis focused on identifying potential measures to improve original STPA. Even though the modified STPA approach has shown its advancement, however,

the limitations are still nonnegligible. One of the biggest drawback is that, the modified approach is not able to deal with the repetition and complexity of casual factors and safety constraints. It also happens to original STPA with a detail-design phase. Further efforts are required to address on this problem.

7.3 Recommendations for Further Work

According to the current results, recommendations are presented here for possible extensions of future research work.

1. This master thesis conducted a continuous work based on STPA primer. The STPA handbook published in March 2018 put forward a more precise and scientific STPA procedures. One of the future work can be performing a STPA analysis process based on STPA handbook and comparing the main differences.

2. Usually STPA is carried out by a team with both professional knowledge and practical experiences. Hence, for practical application, a more professional STPA method for the fully autonomous vessel control system should be implemented.

3. As one of the new approaches, STPA-Sec[50] is an extension of the System-Theoretic Process Analysis (STPA)[51] that extends the safety analysis method with security considerations. It is interesting to investigate the differences between STPA and its extended method.

4. Unlike FMEA and HAZOP, STPA is not yet quantitative, so it is difficult to determine the severity and priory of UCA and safety constraints. Provided with accident data, STPA method will be more powerful.

5. The repetition and complexity of identified casual factors and safety

constraints is still unsolved. New approach is required to address this problem to reduce analysis time.

6. For a long-term perspective, master thesis should make more frequent communication with other co-workers from Maritime department and Cybernetics department with joint topic on ReVolt.

Appendix A

Acronyms

RAMS Reliability, Availability, Maintainability and Safety

STPA Systems Theoretic Process Analysis

FMEA Failure mode and effects analysis

FMECA Failure modes, effects, and criticality analysis

FFMEA Functional Failure mode and effects analysis

HAZOP Hazard and operability study

CHAZOP$_1$ Control Hazard and operability study

CHAZOP$_2$ Computer Hazard and operability study

PESs Programmable Electronic Systems

STAMP System-Theoretic Accident Model and Processes

UCA Unsafe Control Action

FTA Fault Tree Analysis

P&ID Piping and Instrumentation Diagram

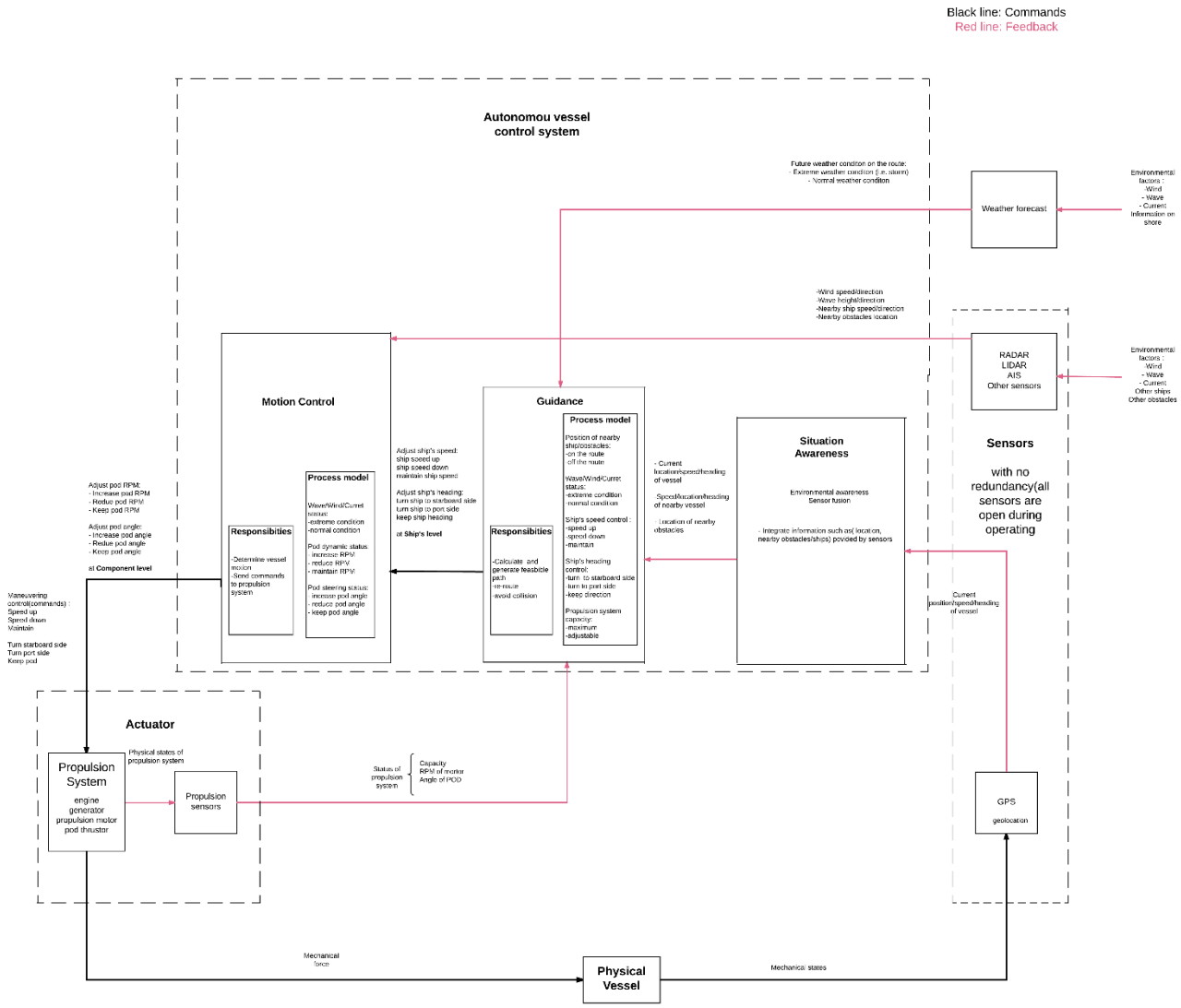
I/O Input/output

AL Autonomy Level

Appendix B

Control loop diagram

Control loop diagram is established in specialization report autumn 2017. Figure 5.1 is partly adapted from control loop diagram that focus on Guidance system only.


Black line: Commands
Red line: Feedback
Autonomou vessel control system
Future weather condtion on the route:
- Extreme weather condition (i.e. storm)
- Normal weather condition
Weather forecast
Environmental factors :
Wind
- Wave
- Current
Information on shore
-Wind speed/direction
-Wave height/direction
-Nearby ship speed/direction
-Nearby obstacles location
RADAR
LIDAR
AIS
Other sensors
Environmental factors :
Wind
- Wave
- Current
Other ships
Other obstacles
Motion Control
Process model
Wave/Wind/Current status:
-extreme condition
-normal condition
Pod dynamic status:
- increase RPM
- reduce RPM
- maintain RPM
Pod steering status:
- increase pod angle
- reduce pod angle
- keep pod angle
Responsibities
-Determine vessel motion
-Send commands to propulsion system
Adjust pod RPM:
- Increase pod RPM
- Redtuc pod RPM
- Keep pod RPM
Adjust pod angle:
- Increase pod angle
- Redue pod angle
- Keep pod angle
at Component level
Maneuvering control(commands) :
Speed up
Spend down
Maintain
Turn starboard side
Turn port side
Keep pod
Adjust ship's speed:
ship soeed up
ship soeed down
maintain ship speed
Adjust ship's heading:
turn ship to starboard side
turn ship to port side
keep ship heading
at Ship's level
Guidance
Process model
Position of nearby ship/obstacles:
-on the route
-off the route
Wave/Wind/Curret status:
-extreme condition
-normal condition
Ship's speed control :
-speed up
-spend down
-maintain
Ship's heading control:
-turn to starboard side
-turn to port side
-keep direction
Propulsion system capacity:
-maximum
-adjustable
Responsibities
-Calculate and generate feasbible path
-re-route
-avoid collision
- Current location/speed/heading of vessel
- Speed/location/heading of nearby vessel
- Location of nearby obstacles
Situation Awareness
Environmental awareness
Sensor fusion
- Integrate information such as(location, nearby obstacles/ships) povided by sensors
Sensors
with no redundancy(all sensors are open during operating
Current position/speed/heading of vessel
Actuator
Propulsion System
engine
generator
propulsion motor
pod thrustor
Physical states of propulsion system
Propulsion sensors
Status of propulsion system
Capacity
RPM of motor
Angle of POD
GPS
geolocation
Mechanical forces
Physical Vessel
Mechanical states

Bibliography

1. News, D.I.i.t. *What the Future of Autonomy Looks Like for Your Industry*. 2017 [cited 2017 11-16]; Available from: http://dataspeedinc.com/future-autonomy-looks-like-industry/.
2. WARRENDALE. *U.S. Department of Transportation's New Policy on Automated Vehicles Adopts SAE International's Levels of Automation for Defining Driving Automation in On-Road Motor Vehicles*. 2016; Available from: https://www.sae.org/news/3544/.
3. THOMAS, N.G.L.J.P., *STPA HANDBOOK*. 2018.
4. Bologna, S., *Safety applications of programmable electronic systems in the process industry*. IFAC Proceedings Volumes, 1999. **32**(2): p. 8775-8780.
5. ABS. *About us*. 2018; Available from: https://ww2.eagle.org/en.html.
6. Jorgensen, J. *Autonomous Vessels: ABS' Classification Perspective*. 2016; Available from: http://onlinepubs.trb.org/onlinepubs/mb/2016spring/presentations/jorgensen.pdf.
7. Breivik, M., *Topics in Guided Motion Control of Marine Vehicles* in *Department of Engineering Cybernetics*. 2010, NTNU: Trondheim.
8. Udjus, G., et al., *Force Field Identification and Positioning Control of an Autonomous Vessel using Inertial Measurement Units*. 2017, NTNU.
9. Javling, B., J.G. Balchen, and S. Strand, *Modified LQG-Control and Quasi-Dynamic Optimal Control for Nonlinear Multivariable Processes.* IFAC Proceedings Volumes, 1993. **26**(2, Part 4): p. 89-92.
10. Matteo Schiaretti, L.C., and Rudy R. Negenborn, *Survey on Autonomous Surface Vessels: Part II - Categorization of 60 Prototypes and Future Applications*, in *8th International Conference, ICCL 2017*. 2017: Southampton, UK.
11. DNV-GL, Maritime Impact, 2017
12. Erik W. Jakobsen, C.S.M., M. Shahrin Osman and Eirik H. Dyrstad *THE LEADING MARITIME CAPITALS OF THE WORLD 2017*. 2017, MENON, DNV-GL.
13. Sames, P.C., *Unmanned ships on the horizon*. 2018, DNV-GL.
14. MarEx. *Rolls-Royce: Robot Ships Will Be Trading by 2020*. 2016 [cited 2017 11/20]; Available from: https://maritime-executive.com/article/rolls-royce-robot-ships-will-be-trading-by-2020.
15. KONGSBERG. *Autonomous shipping*. 2017 [cited 2017 11/20]; Available from: https://www.km.kongsberg.com/ks/web/nokbg0240.nsf/AllWeb/597733F8A1B8C640C12580AC0049C134?OpenDocument.
16. MUNIN. *The Autonomous Ship*. 2016; Available from: http://www.unmanned-ship.org/munin/about/the-autonomus-ship/.
17. Adams, S.D., *ReVolt- next generation short see shipping*. 2014, DNV-GL.
18. Riley, E.F., S. Steen, and E. Bøckmann, *The potential energy savings by application of a wave foil on the autonomous container vessel ReVolt*. 2015, NTNU.

19. Alfheim, H., et al., *Development of a Dynamic Positioning System for the ReVolt Model Ship*. 2017, NTNU.
20. Rokseth, B., I.B. Utne, and J.E. Vinnem, *A systems approach to risk analysis of maritime operations.* Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability, 2017. **231**(1): p. 53-68.
21. Wingrove, M. *IMO to test safety of autonomous ships*. 2017 [cited 2017 11-12]; Available from: http://www.marinemec.com/news/view,imo-to-test-safety-of-autonomous-ships_48376.htm.
22. Valdez Banda, O.A. and F. Goerlandt, *A STAMP-based approach for designing maritime safety management systems.* Safety Science, 2018. **109**: p. 109-129.
23. Cunningham, D., *Waterborne TP SRA: The Autonomous Ship.* 2014(MUNIN Workshop at SMM).
24. Parasuraman, R., T.B. Sheridan, and C.D. Wickens, *A model for types and levels of human interaction with automation.* Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions on, 2000. **30**(3): p. 286-297.
25. Sheridan, T.B., W.L. Verplank, and L.A.B. Massachusetts Inst Of Tech Cambridge Man-Machine Systems, *Human and Computer Control of Undersea Teleoperators*. 1978.
26. Esa Jokioinen, J.P., Antti kolu, Tero Jokela, Jari Tissari, Ari Passio, *Remote and Autonomous Ships The next steps.* Marine, 2017(AAWA).
27. Register, L.s. *Marine*. 2017 [cited 2017 11/20]; Available from: http://www.lr.org/en/marine/.
28. Leveson, N., *An STPA Primer*. 1 ed. 2013.
29. Sardar Muhammad Sulaman1 · Armin Beer2 · Michael Felderer3, M.H., *Comparison of the FMEA and STPA safety analysis methods–a case study.* Software Qual J, 2017.
30. Asim Abdulkhaleq, S.W., *Experiences with Applying STPA to Software-Intensive Systems in the Automotive Domain*, in *Institute of Software Technology*. University of Stuttgart: Germany.
31. Commission, I.E., *IEC 60812:2006*. 1985.
32. Rausand, M., *Risk assessment : theory, methods, and applications*. 2011, Hoboken, N.J.: Wiley.
33. McDermid, J.A., Nicholson, M., Pumfrey, D.J., Fenelon, P. . *Experience with the application of HAZOP to computer-base95ystems*. in *Proceedings of the 10th Annual Conference on Computer Assurance (COMPASS'95) Systems Integrity, Software Safety and Process Security*. 1995.
34. Burge, S., *The Systems Engineering Tool Box*. BURGE HUGHES WALSH.
35. Kletz, T.A., *"Hazop and Hazan: Identifying and Assessing Process Industry Hazards"*. 1999, Institution of Chemical Engineers: UK.
36. Crawley, F., Preston, M. and Tyler, B., *HAZOP: guide to best practice*. 2nd ed. 2008: Institution of Chemical Engineers.
37. Andow, P., *Guidance of HAZOP procedures for computer-controlled plants*. 1991, Health & Safety Executive contract research.
38. Cameron, I.T. and R. Raman, *Process systems risk management*. 2005, Elsevier: Amsterdam.
39. Schubach, S., *A modified computer hazard and operability study procedure* 1997, New South Wales: Australia

40. Martorell, S., et al., *Safety, reliability and risk analysis : theory, methods and applications : proceedings of the European Safety and Reliability Conference, ESREL 2008, and 17th SRA-Europe, Valencia, Spain, September, 22-25, 2008 : Vol. 4*. Vol. Vol. 4. 2009, Boca Raton, Fla: CRC Press.
41. PhD, P.C., *INTRODUCTION TO CHAZOP: ASSESSING THE RISKS OF CONTROL SYSTEM FAILURE*. 2016, Managing Director, xSeriCon.
42. Kletz, T. and E. Institution of Chemical, *Computer control and human error*. 1995, Rugby: Institution of Chemical Engineers.
43. Burns, D.a.P., R.M., *A modified HAZOP methodology for safety critical system assessment.* Directions in Safety-Critical Systems: Proceedings of the Safety-Critical Systems Symposium, 1993(Springer-Verlag, London).
44. Defence, M.o., *A Guideline for HAZOP Studies on Systems Which Include a Programmable Electronic System*. 1995, MOD, Directorate of Standardization: Glasgow, UK.
45. Lear, J.B., *Implementing Safe, Operable Control Systems*. 1995.
46. Nimmo, I., Nunns, S. R. Eddershaw, B. W., *Loss Prevention Bulletin*, I.o.C. Engineers, Editor. 1993.
47. Executive, H.a.S., *Human factors: Managing human failures*. 2018.
48. Thomas, J. and E. United States. Department Of, *Extending and automating a Systems-Theoretic hazard analysis for requirements generation and analysis*. 2012, Sandia National Laboratories.
49. BERTRAM, V., *Towards Unmanned Ships*. 2013, DNV-GL.
50. Young, W., Leveson, N., *Systems thinking for safety and security.* Proceeding ACSAC 2013(ACM Press).
51. Leveson, N., *A new accident model for engineering safer systems.* Safety Science, 2004. **42**(4): p. 237-270.