**Course assignment**

The assignment consists of 3 different sections. In the first section (A), the students are required to select and implement one of the three traditional hazard analysis methods discussed in class and apply the method to a Dynamic Positioning system as explained in this document. In the second section (B), you are required to implement a new hazard analysis method known as System’s Theoretic Process Analysis (STPA) on the same Dynamic Positioning system. Finally, in the third section (C), the students are required to discuss and summarize the experience of applying traditional hazard analysis and STPA.

The assignment can be done in a group (max 3) or individually as preferred. The assignment results must be uploaded in a report format before 17.10.2023 22:00 to Mycourses submission box.

The following applies to the report:

* Cover page with relevant picture, title, name of the team member and their relevant codes, date of submission, supervisor name and teaching assistants names, course name and code and no page number on the cover page should be provided.
* Table of contents should be on a separate page.
* On separate page start section A, B, C.
* Section A, B, C and tasks names should be considered as headings (and part of contents table).
* Headings should be highlighted differently from the text.
* Table captions above the tables, figure captions below the figures.
* Word or Pdf format should be used for submission (Not LaTex).
* Text should be readable.
* Any of three styles (Arial, Calibri, Times New Romans) can be used, but not others.

Section A: Hazard analysis using traditional methods.

This assignment aims to learn the process of implementing traditional methods for identifying hazards in the system. The system under assessment will be described as a separate document. The students can apply any of the three mentioned methods in this section. The tasks for each of these methods are explained below:

I. Hazard analysis using Hazard and Operability study (HAZOP)

**Task 1: Describe the system under assessment (system structure and processes).**

The system and activities under assessment must be described. The description should include an introduction, system operation, components and component’s intended function. As the focus of this method is about identifying how the system components might deviate from its normal function, it is important to clearly define the intended functions of each components.

**Task 2: Identify the functional parameters of the system components.**

Next, the parameters that affect the functions of each system components need to be identified.

For example:

Table Components and functional parameters.

|  |  |
| --- | --- |
| **Components and functions** | **Functional parameters** |
| Alarm unit | Sound intensity |
| Generator | Power |

**Task 3: Identify deviations using guidewords.**

The functional parameters identified in previous steps should then be combined with the guidewords to identify the possible deviations. There are 7 different guidewords that can be used for this task which are available and explained in lecture slides.

For example:

Table Deviations identified using guidewords.

|  |  |  |  |
| --- | --- | --- | --- |
| **Components and functions** | **Functional parameters** | **Guidewords** | **Deviation** |
| Alarm unit | Sound intensity | None | No sound generated from an alarm unit. |
|  | Sound intensity | Less | Less sound intensity from an alarm unit than designed. |

**Task 4: Determine the effects and potential causes of the developed deviations**

Next, the effects due to the developed deviation and the causes resulting in the deviation should be determined. The causes can include component failures, human errors, software issues and interaction issues.

For example:

Table HAZOP table without safety controls.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Components and functions** | **Functional parameters** | **Guidewords** | **Deviation** | **Consequence** | **Cause** |
| Alarm unit | Sound  intensity | None | No sound generated  from an alarm unit. | The alarm doesn’t trigger when the  vessel positioning or heading highly deviates. | The power supply system fails resulting in a power cut during the operation.  The limits set on computer for alarms are incorrect. |
| Alarm unit | Sound  intensity | Less | Less sound intensity  from an alarm unit than designed. | The alarm is not heard by the distant operator | The alarm sound settings or speaker settings are not set to recommended settings. |

**Task 5: Define safety controls for mitigating the consequences and potential causes.**

After identifying the causes of system deviations, the safety controls for the system must be defined. These safety controls could include creating procedures, adding safety components etc to mitigate the cause of the deviations or to control the consequences when the deviations occurs.

For example:

Table Complete HAZOP table.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Components and functions** | **Functional parameters** | **Guide words** | **Deviation** | **Consequence** | **Cause** | **Safety control** |
| Alarm unit | Sound  intensity | None | No sound generated  from an alarm unit. | The alarm  doesn’t  trigger when the vessel positioning or heading highly deviates. | The power supply system fails resulting in a power cut during the operation.  The limits set on computer for alarms are incorrect. | A UPS must be available for alarm unit in case of power cuts.  The limits set for alarm unit must be checked by operator before initiating the operation. |
|  | Sound  intensity | Less | Less sound intensity  from an alarm unit than designed. | The alarm is not heard by the distant operator | The alarm sound settings or speaker settings are not set to recommended settings. | The alarm settings or speaker settings must be checked by operator before initiating the operation. |

II. Hazard analysis using Failure Mode and Effect Analysis (FMEA)

**Task 1: Define the system and activities under assessment (system structure and processes).**

The system and activities under assessment must be described. The description should include an introduction, system operation, components and component’s intended function. As the focus of this method is about assessing the failure modes of system components, it is important to clearly define the functions of each components.

**Task 2: Identify the failure modes of each of the components and its functions.**

Next, the failure modes for each of the components and its functions needs to be identified.

For example:

Table FMEA failure modes.

|  |  |  |
| --- | --- | --- |
| **Components** | **Function** | **Failure modes** |
| Generator | To provide power to the DP system and its components | Generator shuts down during DP  operation |

**Task 3: Determine the effects and potential causes of the failure modes.**

After identifying the failure modes, the effects and potential causes of the failure modes must be determined. The causes can include component failures, human errors, software issues and interaction issues.

For example:

Table FMEA table without safety controls.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Components** | **Function** | **Failure modes** | **Effects** | **Causes** |
| Generator | To provide power to the DP system and its components | Generator shuts down during DP  operation | The vessel will experience a blackout which can result to loss of mission or vessel. | Low level of coolant due to an external or internal leakage. |

**Task 4: Define safety controls for mitigating the consequences and potential causes.**

After identifying the causes of failure modes, the safety controls for the system must be defined. These safety controls could include creating procedures, adding safety components etc to mitigate the causes of the failure mode or to control the consequences when the failure mode occurs.

Table Complete FMEA table.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Compone**  **nts** | **Function** | **Failure modes** | **Consequences** | **Causes** | **Safety controls** |
| Generator | To provide power to the DP system and its  components | Generator shuts down during DP operation | The vessel will experience a blackout which can result to loss of mission or vessel. | Low level of coolant due to an external or internal leakage. | Weekly inspection of generator to notice any visible coolant leakage. |

III. Hazard analysis using Fault Tree Analysis (FTA)

**Task 1: Describe the system under assessment (system structure and processes).**

The system and activities under assessment must be described. The description should include an introduction, operation, components and component’s intended function. As the focus of this methods is to identify the events that can lead to a system fault, it is important to clearly define the components and the functions.

**Task 2: Identify the combination of causes that can lead to the system-level fault or loss.**

Next, the system-level fault and the events that can lead to the system-level fault must be identified. The combinations of events should be demonstrated using suitable symbols (types of symbols and its details are available in lecture slides).

For example:

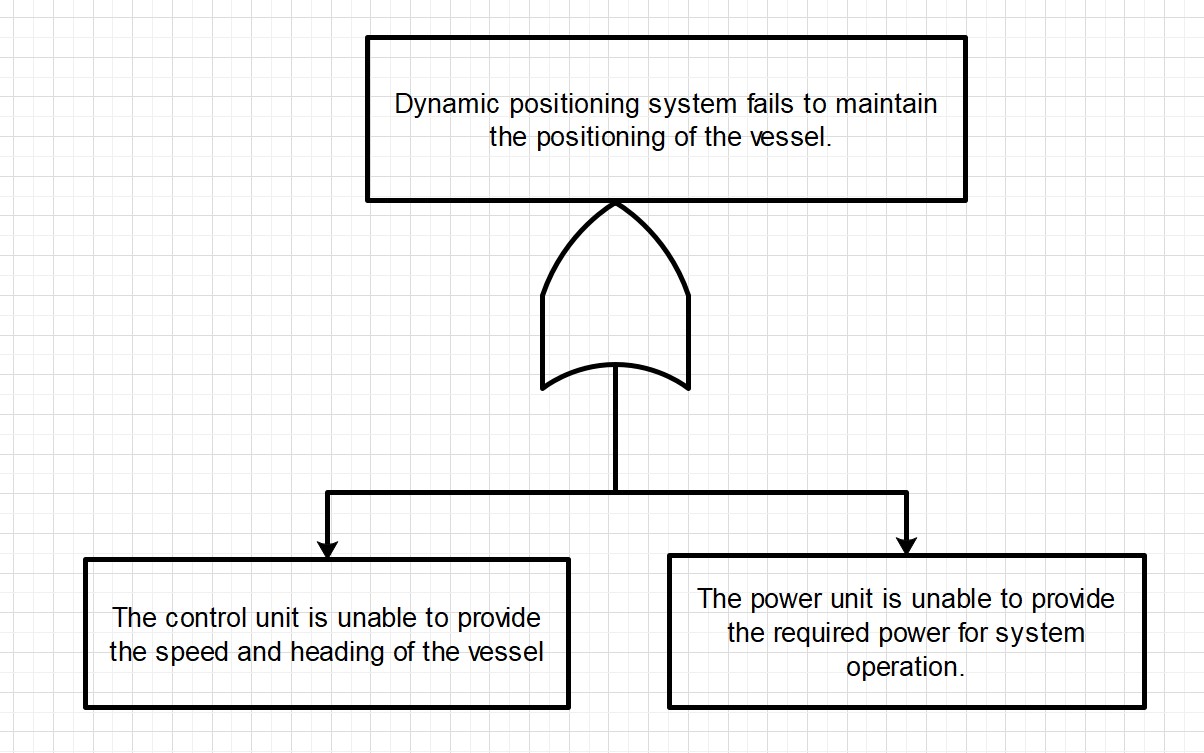


Figure Initial Fault Tree.

**Task 3: Continue developing the fault tree until the basic causes or events leading to the fault are found.**

The fault tree should then be developed further until the basic causes or events are reached. For this assignment, minimum of 4 layers of hierarchy including the system-level fault is required.

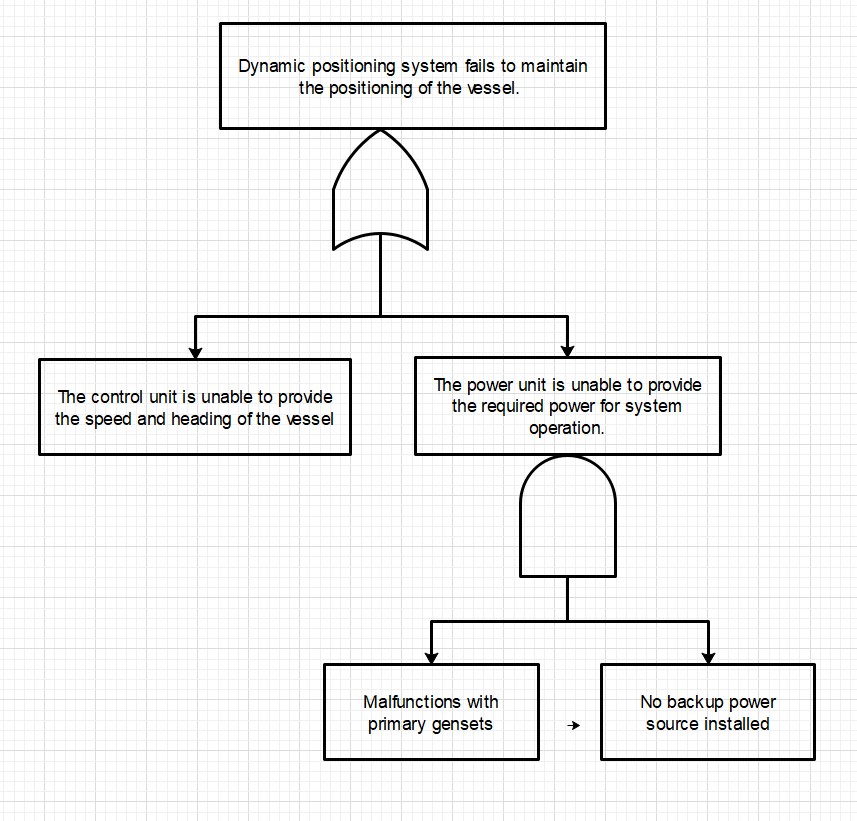


Figure Developed Fault Tree.

**Task 4: Define safety controls for mitigating the potential faults.**

Finally, the safety controls for each of the basic causes or events needs to be defined. These safety controls could include creating procedures, adding safety components etc to mitigate the causes of the failure mode or to control the consequences when the failure mode occurs.

For example:

Malfunctions with primary gensets: The coolant level and oil level should be regularly inspected to avoid sudden malfunctions.

Section B: Hazard analysis using System’s Theoretical Process Analysis (STPA).

The aim of this assignment is to learn the process of implementing STPA for identifying hazards in the system. The description of the system under assessment and the detailed guidelines of STPA process will be provided as separate documents. There are eight different tasks in this assignment and are explained below:

1. Define the losses.
2. Identify the system-level hazards.
3. Create safety constraints/requirements for the system-level hazards.
4. Create the control structure of the system.
5. Identify control actions that can be potentially unsafe.
6. Identify the causes of Unsafe control actions.
7. Define safety controls to prevent the causes.
8. Present the results of the analysis.

**Task 1: Define the losses.**

The losses to be covered in the analysis must be presented in this section. These losses may include the loss of life or human injury, financial loss, loss of mission, environmental pollution, loss of reputation, leak of information etc.

For example:

L1: Loss of mission.

L2: Loss of life or human injury

**Task 2: Identify the system-level hazards.**

Next, the hazards associated to each loss must be identified. For ensuring the effectivity of this analysis, only the system level hazards must be included. This allows us to start the analysis with wider scope. The identification of component failures, software errors, design errors, and other causes leading to the systemic hazards and losses shouldn’t be included in this step as it will be identified in final steps of this analysis.

For specifying these system-level hazards, the following format is suggested in STPA handbook: <Hazard specification> = <System> & <Unsafe condition> & <Link to the resulting losses>

For example:

H-1 = The DP system doesn’t maintain the positioning of the vessel during navigation. (L-1, L-2)

**Task 3: Create safety constraints/requirements for the system-level hazards.**

In this task, the safety constraints or requirements for preventing the system-level hazards, must be defined. It can be simply achieved by using the following format as suggested in STPA handbook: <Safety constraint specification> = <System> & <Condition to enforce> & <Link to hazards> For example:

SC-1 = The DP system must maintain the specified positioning of the vessel during the navigation. (H1)

**Task 4: Create a control structure of the system.**

Next, a control structure of the system should be created. This control structure should present all the interactions (control actions and feedback) between the controllers and controlled processes of the system. Figure 3 shows an example of a control structure, where the texts (blue) in down arrows represent the control actions of the controllers and the texts (green) in up arrows represent the feedback that the controllers receive from the controlled processes.

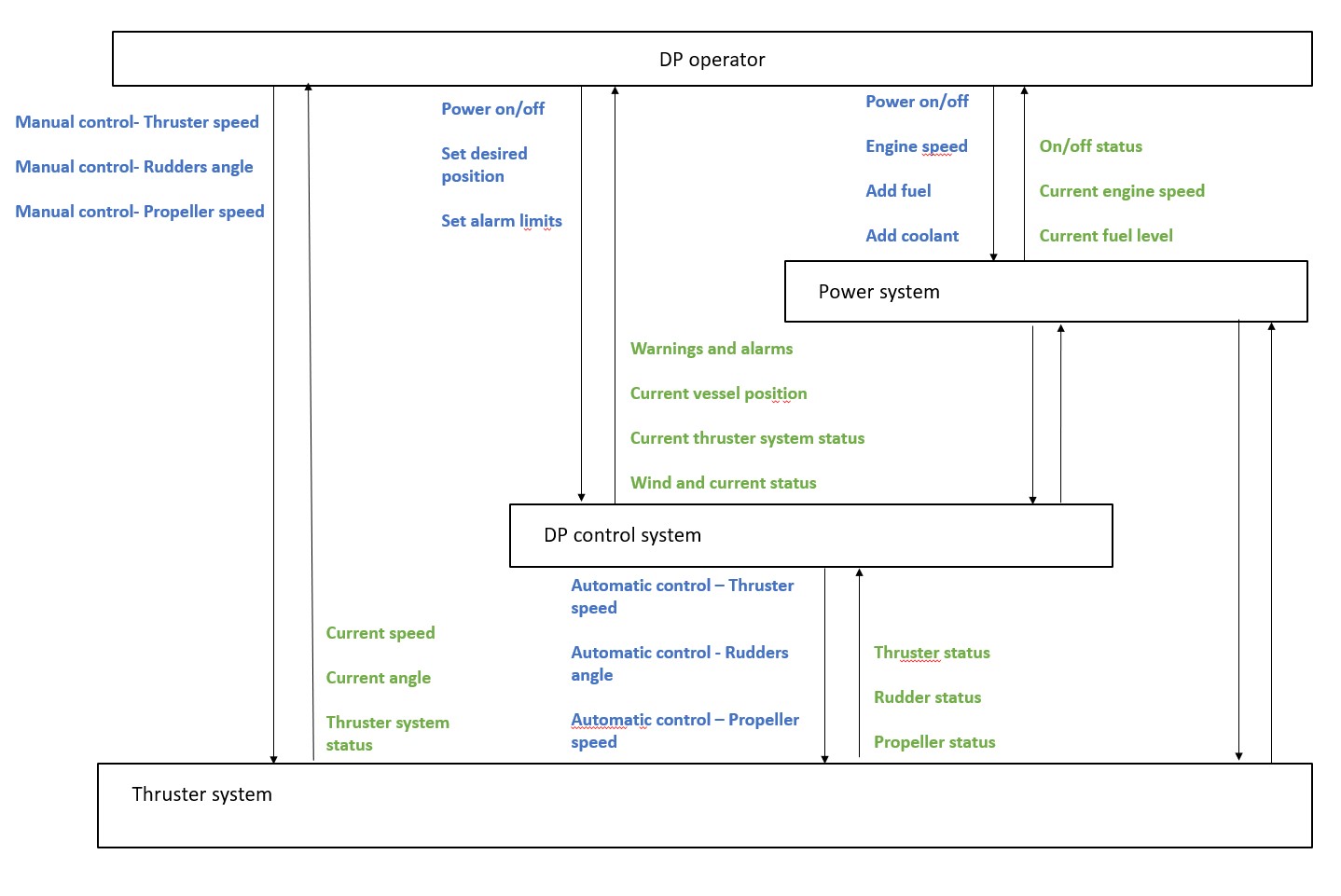


Figure An example of STPA control structure for DP operation.

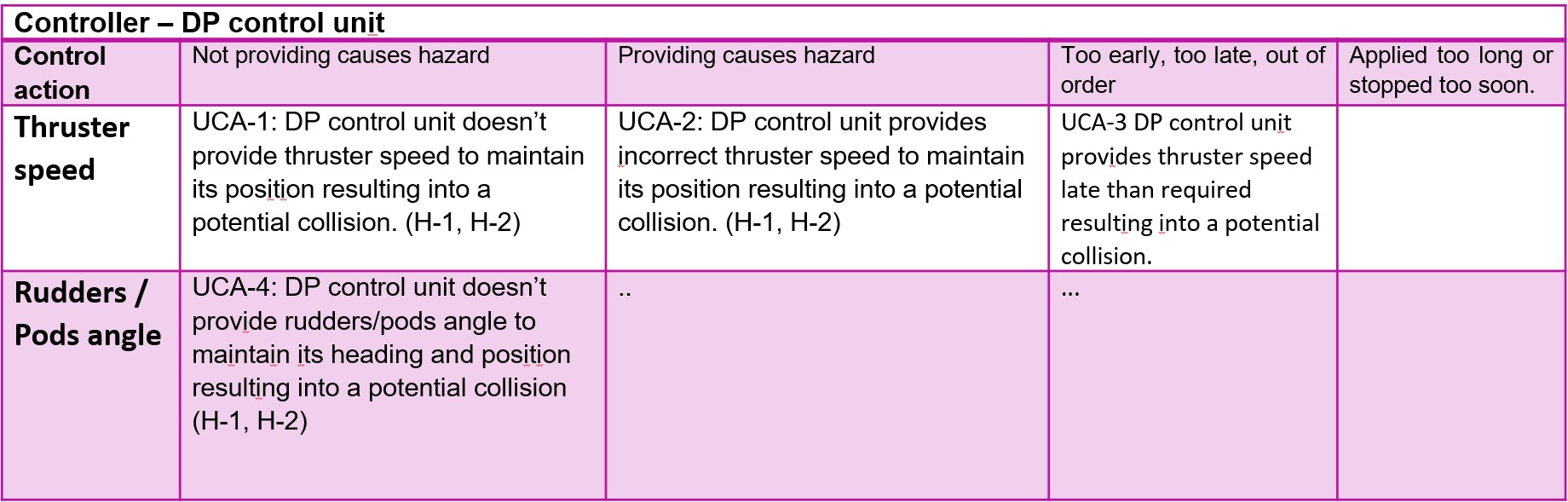
**Task 5: Identify Unsafe Control Actions (UCA’s).**

After creating the control structure, the control actions that are potentially unsafe should be identified. This can be done by identifying the unsafe scenarios for each control action using the following guidewords:

1. Not providing the control action leads to a hazard.
2. Providing the control action leads to a hazard
3. Providing the control action too early, too late or in the wrong order leads to a hazard 4. Providing the control action for too long or if stopped too soon leads to a hazard.

The identified UCA’s should be specified with the source (or controller), the control action, the context in which it happens and the link to the resulting hazards. Table 8 shows an example of identifying unsafe scenarios for a control action “steering angle command” under the controller DP Control Unit from Figure 1.

Table Identify the UCA’s for Thruster speed, Rudders/Pods angle control action.



**Task 6: Identify the causes or scenarios of potential UCA’s.**

Next for each potential UCA’s, the causes of its occurrence should be identified. This is achieved by considering the following two scenarios:

1. Why would Unsafe Control Action’s occur?
2. Why would the control actions be improperly executed or not executed, leading to hazards? For example, the causes identified for UCA-1 from Table 1 are as follows:

**UCA-1: DP control unit doesn’t provide thruster speed to maintain its position resulting into a potential collision. (H-2, H-3)**

**Component failures:**

* The motion reference units fail to provide required input to calculate the thruster speed.
* The servo actuators or controllers fails to implement the thruster speed.

**Inadequate control algorithm (software errors):**

* The DP control unit and Kalman filters are not able to process the data from the motion reference units.
* The DP system is not able to calculate the required thruster speed to maintain the vessel positioning.

**Task 7: Define safety controls.**

In this task, the safety controls for avoiding the causes identified for each UCA’s should be defined. These safety controls can include controller requirements, design changes, operational requirements, safeguards etc.

For example:

* Secondary MRU units should be made available in case Primary MRU fails to provide required motion information.
* Failsafe options should be implemented in case of emergency situations. For example, the vessel should maintain the previous position in such situations until the MRU is able to provide the required data or until the operator takes manual control.
* Alarms should be generated to the operator notifying the situation.

**Task 8: Present the results of the analysis.**

Finally, the results of this assignment should be clearly presented. There is no specific format or guidelines for this task. Thus, what to present and how to present as the outcome of this analysis should be decided by the students themselves.

Section C: Discuss and summarize the experience of applying traditional hazard analysis and STPA.

In this section, the summary of the assignment experience needs to be provided. The students should provide the differences and similarities found between the two methods. Furthermore, the advantages and disadvantages of each methods based on the assignment experience must be reported.

**Detailed guidelines of the STPA process is available through the link provided below:**

<http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf>

**The system description for the assignment will be uploaded to the Mycourses website.**