1 Unsafe Control Actions

Table 1: UCA

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Incorrect Timing/ Incorrect Order	Stopped Too Soon/ Applied Too Long
Customer Destination Command	**UCA1.1** Customer not monitor the potential environmental risks. **UCA1.2** No operator feedback to customer.	**UCA1.3** Respond to emergency situations not in time.	**UCA1.4** Destination command occurring too late.	**UCA1.5** Repeatedly passing commands.
Operator Passing Command	**UCA2.1** Operator not monitor the potential environmental risks. **UCA2.2** Software component not back to information. **2.3** No command passing to global path planning component.	**UCA2.4** Respond to emergency situations not in time. **UCA2.5** Global path planning component received command delayed.	**UCA2.6** Destination command occurring too late. **UCA2.7** Global path planning component received wrong/incorrect command.	**UCA2.8** Repeatedly passing commands.
Key Command from Software to Hardware	**UCA3.1** No command from software to hardware component/ localisation component.	**UCA3.2** Hardware component response delay.	**UCA3.3** Key command occurring too late. **UCA3.4** Hardware component received command in incorrect timing.	**UCA3.5** Hardware authorisation applied time too long
Hardware Authorisation Command to sensors	**UCA4.1** Sensor issues lead to not get the command	**UCA4.2** Sensor broken/ not response.	**UCA4.3** Sensor response too late/ in correct timing.	**UCA4.4** Sensor stopped too soon.

Continued

Supervisor Prior Knowledge	**UCA5.1** Default map/ known obstacles not be received by global path planning component.	**UCA5.2** Information received not in time.	**UCA5.3** Information passing in the incorrect timing.	**UCA5.4** Global path planning component still received prior knowledge.
Change Information between Global Path Planning and Local Path Planning components	**UCA6.1** Waypoint information not be received **UCA6.2** No request new path plan.	**UCA6.3** Local path planning component issues/ not responds.	**UCA6.4** Global path planning component has incorrect passing information timing.	**UCA6.5** Local path planning component has applied too long.
Sensors get environmental data from world	**UCA7.1**Sensors issues/ broken. **UCA7.2** Do not get environmental data.	**UCA7.3** Sensors not get data in time.	**UCA7.4** Sensors not have completed data.	**UCA7.5** Sensors stopped too soon.
Sensors Transfer Row Data	**UCA8.1** Request command not be received/ Sensors broken.	**UCA8.2** Data transmission too slow. **UCA8.3** Obstacle detection model received data too slow.	**UCA8.4** Only part of data has transferred in model.	**UCA8.5** Only part of data has transferred in model. **UCA8.6** Sensors stopped too soon.
Localisation	**UCA9.1** Not received the input information from sensors and hardware authorisation.	**UCA9.2** Processing information is not timely.	**UCA9.3** Information output/ feedback is incorrect timing.	**UCA9.4** Localisation information stopped too soon.
	Wrong/Invalid/Incomplete/Perturbed			
	UCA9-1.1 Wrong setting and model design. **UCA9-1.2** Incomplete/ invalid data makes wrong mapping. **UCA9-1.3** Image feature segmentation has low accuracy. **UCA9-1.4** Feature localization has low accuracy. **UCA9-1.5** Location data fusion suffered perturbed.			
Obstacle Detection Model	**UCA10.1** Row data not be sent into the model.	**UCA10.2** Data transmission is unstable.	**UCA10.3** Data transmission at incorrect timing	**UCA10.4** Data stopped before being fully fed into the model.
	Wrong/Invalid/Incomplete/Perturbed/Incapable			

Continued

	UCA10-1.1 Wrong hyperparameter setting and model design. **UCA10-1.2** Incomplete/ invalid data makes wrong data pre-process. **UCA10-1.3** Incomplete/ invalid setting of the hyperparameter. **UCA10-1.4** Model suffered perturbed. **UCA10-1.5** Incomplete/ invalid validation and verification.			
	UCA10-2.1 Wrong hyperparameter setting and model design. **UCA10-2.2** Data with wrong labels. **UCA10-2.3** Data was perturbed by external attackers. **UCA10-2.4** Model suffered perturbed. **UCA10-2.5** Incomplete/ invalid testing. **UCA10-2.6** Convolutional layer training not well. **UCA10-2.7** Non-max suppression layer selection is unreasonable.			
Key Command for Action from Local Path Planning	**UCA11.1** No command from local path planning component	**UCA11.2** Kinematic model response delay.	**UCA11.3** Key command occurring too late.	**UCA11.4** Kinematic model applied time too long.
Request Command to Actuation System	**UCA12.1** No command from Kinematic model to actuation system.	**UCA12.2** Actuation system response delay.	**UCA12.3** Key command occurring too late.	**UCA12.4** Actuation system applied time too long.

Continued

Actuation System control AUV actions	**UCA13.1** AUV management system do not passing command to steering/Power/brake unit. **UCA13.2** AUV management system do not passing command to monitor/measurement unit. **UCA13.3** Rotation/Position unit do not send command to hardware. **UCA13.4** Rotation/Position unit do not sent feedback to monitor.	**UCA13.5** Each unit/monitor response delay.	**UCA13.6** Key command occurring too late.	**UCA13.7** AUV condition monitor/ motor applied time too long.
AUV Action Interact	**UCA14.1** No feedback to world or other components	**UCA14.2** Sent information is not timely to other components.	**UCa14.3** Feedback occurring too late.	**UCA14.4** Feedback information is incomplete.

2 Causal Scenarios

UCA1.1 Customer not monitor the potential environmental risks.

- Customer is not able to predict future states of the environment and therefore ignore environmental risks.
- Insufficient feedback from the operator for the customer not to monitor the potential environmental risks.

UCA1.2 No operator feedback to customer.

- Insufficient feedback from the operator for the customer not to monitor the potential environmental risks.

UCA1.3 Respond to emergency situations not in time.

- Insufficient feedback from the operator for the customer not to monitor the potential environmental risks.

UCA1.4 Destination command occurring too late.

- Customer is not able to predict future states of the environment and therefore ignore environmental risks.

UCA1.5 Repeatedly passing commands.

- Customer is not able to predict future states of the environment and therefore ignore environmental risks.
- Insufficient feedback from the operator for the customer not to monitor the potential environmental risks.

UCA2.1 Operator not monitor the potential environmental risks.

- Operator is not able to predict future states of the environment and therefore ignore environmental risks.
- Insufficient feedback from the operator for the customer not to monitor the potential environmental risks.

UCA2.2 Software component not back to information.

- No data/information passing between components.

UCA2.3 No command passing to global path planning component.

- No data/information passing between components.

UCA2.4 Respond to emergency situations not in time.

- Operator is not able to predict future states of the environment and therefore ignore environmental risks.

UCA2.5 Global path planning component received command delayed.

- Data transmission is unstable.
- Components receive unit delay/issues.

UCA2.6 Destination command occurring too late.

- Data transmission is unstable.
- Components receive unit delay/issues.

UCA2.7 Global path planning component received wrong/incorrect command.

- Data transmission is unstable.

- Operator mistake to passing wrong command.

UCA2.8 Repeatedly passing commands.

- Operator mistake to Repeatedly passing commands.

UCA3.1 No command from software to hardware component/ localisation component.

- Data transmission is unstable.
- Components receive unit delay/issues.

UCA3.2 Hardware component response delay.

- Components receive unit delay/issues.

UCA3.3 Key command occurring too late.

- Components receive unit delay/issues.

UCA3.4 Hardware component received command in incorrect timing.

- Data transmission is unstable.

UCA3.5 Hardware authorisation applied time too long.

- Data transmission is unstable.
- Component issues/ part of units broken.

UCA4.1 Sensor issues lead to not get the command.

- Component issues/ part of units broken.

UCA4.2 Sensor broken/ not response.

- Component issues/ part of units broken.

UCA4.3 Sensor response too late/ in correct timing.

- Data transmission is unstable.
- Component issues/ part of units broken.

UCA4.4 Sensor stopped too soon.

- Data transmission is unstable.

UCA5.1 Default map/ known obstacles not be received by global path planning component.

- Data transmission is unstable.
- Operator mistake to passing wrong information.

UCA5.2 Information received not in time.

- Information transmission is unstable.

UCA5.3 Information passing in the incorrect timing.

- Information transmission is unstable.

UCA5.4 Global path planning component still received prior knowledge.

- Feedback information transmission is unstable.

UCA6.1 Way-point information not be received

- Information transmission is unstable.

UCA6.2 No request new path plan.

- Information transmission is broken/interrupt.

UCA6.3 Local path planning component issues/ not responds.

- Information transmission is broken/interrupt.

UCA6.4 Global path planning component has incorrect passing information timing.

- Information transmission is broken/interrupt.
- Data transmission is unstable.

UCA6.5 Local path planning component has applied too long.

- Information transmission is broken/interrupt.
- Data transmission is unstable.

UCA7.1 Sensors issues/ broken.

- No data from sensors (transient/ permanent)
- Corrupted sensor data passing.

UCA7.2 Do not get environmental data.

- Sensors issues/ broken.
- No command passing to sensors.

UCA7.3 Sensors not get data in time.

- Sensors issues/ broken.
- Data transmission is unstable.

UCA7.4 Sensors not have completed data.

- Sensors issues/ broken.
- Data transmission is unstable.

UCA7.5 Sensors stopped too soon.

- Sensors issues/ broken.
- Data transmission is unstable.

UCA8.1 Request command not be received/ Sensors broken.

- Data transmission is unstable.

UCA8.2 Data transmission too slow.

- Components issues/ broken.

UCA8.3 Obstacle detection model received data too slow.

- Data transmission is unstable.
- Components receive unit delay/issues.

UCA8.4 Only part of data has transferred in model.

- Components issues/ broken.
- Sensors issues/ broken.
- Data transmission is unstable.

UCA8.5 Only part of data has transferred in model.

- Components issues/ broken.
- Sensors issues/ broken.
- Data transmission is unstable.

UCA8.6 Sensors stopped too soon.

- Data transmission is unstable.
- Information transmission is broken/interrupt.

UCA9.1 Not received the input information from sensors and hardware authorisation.

- Data transmission is unstable.
- Components receive unit delay/issues.

UCA9.2 Processing information is not timely.

- Data transmission is unstable.

- Components receive unit delay/issues.

UCA9.3 Information output/ feedback is incorrect timing.

- Data transmission is unstable.
- Components receive unit delay/issues.

UCA9.4 Localisation information stopped too soon.

- Data transmission is unstable.
- Components receive unit delay/issues.

UCA9-1.1 Wrong hyperparameter setting and model design.

- Programmer mistake.
- programmer lacking experience.

UCA9-1.2 Incomplete/ invalid data makes wrong mapping.

- Data transmission is unstable.
- Model receive unit issues.
- Raw data oversize/ unacceptable.

UCA9-1.3 Image feature segmentation has low accuracy.

- Function setting unreasonable/ mistake.

UCA9-1.4 Feature localization has low accuracy.

- Function setting unreasonable/ mistake.

UCA9-1.5 Location data fusion suffered perturbed.

- Attacks encountered during data pre-process.

UCA10.1 Row data not be sent into the model.

- Data transmission is unstable.
- Model receive unit issues.
- Raw data oversize/ unacceptable.

UCA10.2 Data transmission is unstable.

- Model receive unit issues.
- Raw data oversize/ unacceptable.

UCA10.3 Data transmission at incorrect timing

- Information transmission is broken/interrupt.
- Data transmission is unstable.

UCA10.4 Data stopped before being fully fed into the model.

- Data transmission is unstable.
- Components receive unit delay/issues.

UCA10-1.1 Wrong hyperparameter setting and model design.

- Programmer mistake.
- programmer not lacking experience.

UCA10-1.2 Incomplete/ invalid data makes wrong data pre-process.

- Data transmission is unstable.
- Model receive unit issues.
- Raw data oversize/ unacceptable.

UCA10-1.3 Incomplete/ invalid setting of the hyper-parameter.

- Data transmission is unstable.
- Hyperparameter setting wrong.
- programmer not lacking experience.

UCA10-1.4 Model suffered perturbed.

- Attacks encountered during testing model.

UCA10-1.5 Incomplete/ invalid validation and verification.

- Validation and verification with wrong methods.
- Model testing issues.

UCA10-2.1 Wrong hyperparameter setting and model design.

- Programmer mistake.
- programmer lacking experience.

UCA10-2.2 Data with wrong labels.

- Part of data missing labelling.
- Part of data not be labelled.

UCA10-2.3 Data was perturbed by external attackers.

- Attacks encountered during data processing.

UCA10-2.4 Model suffered perturbed.

- Attacks encountered during testing model.

UCA10-2.5 Incomplete/ invalid testing.

- Testing unreasonable/ mistake.

UCA10-2.6 Convolutional layer training not well.

- Uneven distribution of data features.

UCA10-2.7 Non-max suppression layer selection is unreasonable.

-

UCA11.1 No command from local path planning component.

- Command transmission is unstable.
- Components receive unit delay/issues.

UCA11.2 Kinematic model response delay.

- Information transmission is unstable.

UCA11.3 Key command occurring too late.

- Information transmission is unstable.

UCA11.4 Kinematic model applied time too long.

- Information transmission is unstable.

UCA12.1 No command from Kinematic model to actuation system.

- Command transmission is unstable.
- Components receive unit delay/issues.

UCA12.2 Actuation system response delay.

- Information transmission is unstable.

UCA12.3 Key command occurring too late.

- Information transmission is unstable.

UCA12.4 Actuation system applied time too long.

- Information transmission is unstable.

UCA13.1 AUV management system do not passing command to steering/Power/brake unit.

- Command transmission is unstable.
- Components receive unit delay/issues.

UCA13.2 AUV management system do not passing command to monitor/measurement unit.

- Command transmission is unstable.
- Components receive unit delay/issues.

UCA13.3 Rotation/Position unit do not send command to hardware.

- Command transmission is unstable.
- Components receive unit delay/issues.

UCA13.4 Rotation/Position unit do not sent feedback to monitor.

- Command transmission is unstable.
- Components receive unit delay/issues.

UCA13.5 Each unit/monitor response delay.

- Information transmission is unstable.

UCA13.6 Key command occurring too late.

- Information transmission is unstable.

UCA13.7 AUV condition monitor/ motor applied time too long.

- Information transmission is unstable.

UCA14.1 No feedback to world or other components

- Command transmission is unstable.
- Components receive unit delay/issues.

UCA14.2 Sent information is not timely to other components.

- Command transmission is wrong.

UCa14.3 Feedback occurring too late.

- Information transmission is unstable.

UCA14.4 Feedback information is incomplete.

- Information transmission is unstable.

3 Safety requirement

UCA1.1 Customer does not monitor the potential environmental risks.

- Because predicting future states of the entire environment is a difficult cognitive task, predictive aids will likely be required.

UCA1.2 No operator feedback to customer.

- System shall indicate the operator current communication status.

UCA1.3 Respond to emergency situations not in time.

- Insufficient feedback from the operator for the customer not to monitor the potential environmental risks.

UCA1.4 Destination command occurring too late.

- Monitor systems should be used normal situations.

UCA1.5 Repeatedly passing commands.

-

- Monitor systems should be used normal situations.

UCA2.1 Operator does not monitor the potential environmental risks.

- Because predicting future states of the entire environment is a difficult cognitive task, predictive aids will likely be required.

UCA2.2 Software component not back to information.

- Monitor systems should be used normal situations.

-

UCA2.3 No command passing to global path planning component.

- Monitor systems should be used normal situations.

UCA2.4 Respond to emergency situations not in time.

- Monitor systems should be used normal situations.

UCA2.5 Global path planning component received command delayed.

- Monitor systems should be used normal situations.

UCA2.6 Destination command occurring too late.

- Monitor systems should be used normal situations.

UCA2.7 Global path planning component received wrong/incorrect command.

- Monitor systems should be used normal situations.

UCA2.8 Repeatedly passing commands.

- Monitor systems should be used normal situations.

UCA3.1 No command from software to hardware component/ localisation component.

- Monitor systems should be used normal situations.

UCA3.2 Hardware component response delay.

- Monitor systems should be used normal situations.

UCA3.3 Key command occurring too late.

- Monitor systems should be used normal situations.

UCA3.4 Hardware component received command in incorrect timing.

- Monitor systems should be used normal situations.

UCA3.5 Hardware authorisation applied time too long.

- Monitor systems should be used normal situations.

UCA4.1 Sensor issues lead to not get the command.

- Monitor systems should be used normal situations.

UCA4.2 Sensor broken/ no response.

- Monitor systems should be used normal situations.

UCA4.3 Sensor response too late/ in correct timing.

- Monitor systems should be used normal situations.

UCA4.4 Sensor stopped too soon.

- Monitor systems should be used normal situations.

UCA5.1 Default map/ known obstacles not be received by global path planning component.

- Monitor systems should be used normal situations.

UCA5.2 Information received not in time.

- Monitor systems should be used normal situations.

UCA5.3 Information passing in the incorrect timing.

- Monitor systems should be used normal situations.

UCA5.4 Global path planning component still received prior knowledge.

- Monitor systems should be used normal situations.

UCA6.1 Way-point information not be received

- Monitor systems should be used normal situations.

UCA6.2 No request for new path plan.

- Monitor systems should be used normal situations.

UCA6.3 Local path planning component issues/ not responds.

- Monitor systems should be used normal situations.

UCA6.4 Global path planning component has incorrect passing information timing.

- Monitor systems should be used normal situations.

UCA6.5 Local path planning component has applied too long.

- Monitor systems should be used normal situations.

UCA7.1 Sensors issues/ broken.

- Monitor systems should be used normal situations.

UCA7.2 Do not get environmental data.

- Monitor systems should be used normal situations.

UCA7.3 Sensors not get data in time.

- Monitor systems should be used normal situations.

UCA7.4 Sensors not have the completed data.

- Monitor systems should be used normal situations.

UCA7.5 Sensors stopped too soon.

- Monitor systems should be used normal situations.

UCA8.1 Request command not be received/ Sensors broken.

- Monitor systems should be used normal situations.

UCA8.2 Data transmission is too slow.

- Monitor systems should be used normal situations.

UCA8.3 Obstacle detection model received data too slowly.

- Monitor systems should be used normal situations.

UCA8.4 Only part of the data has transferred in model.

- Monitor systems should be used normal situations.

UCA8.5 Only part of the data has transferred in model.

- Monitor systems should be used normal situations.

UCA8.6 Sensors stopped too soon.

- Monitor systems should be used normal situations.

UCA9.1 Not received the input information from sensors and hardware authorisation.

- Monitor systems should be used normal situations.

UCA9.2 Processing information is not timely.

- Monitor systems should be used normal situations.

UCA9.3 Information output/ feedback is incorrect timing.

- Monitor systems should be used normal situations.

UCA9.4 Localisation information stopped too soon.

- Monitor systems should be used normal situations.

UCA9-1.1 Wrong hyperparameter setting and model design.

- Monitor systems should be used normal situations.

UCA9-1.2 Incomplete/ invalid data makes wrong mapping.

- Common time(NTP) to synchronise data and results.

UCA9-1.3 Image feature segmentation has low accuracy.

- Classifier accuracy/reliability for critical objects ¿X.

UCA9-1.4 Feature localization has low accuracy.

- Classifier accuracy/reliability for critical objects ¿X.

UCA9-1.5 Location data fusion suffered perturbed.

- Situational awareness.

UCA10.1 Row data not be sent into the model.

- Monitor systems should be used normal situations.

UCA10.2 Data transmission is unstable.

- The driver software for the sensor (such as a wide-angle camera) should enable resolution adjustments.
- Raw data should be compressed during transmission.

UCA10.3 Data transmission at incorrect timing

- Monitor systems should be used normal situations.

UCA10.4 Data stopped before being fully fed into the model.

- Monitor systems should be used normal situations.

UCA10-1.1 Wrong hyperparameter setting and model design.

- Common time(NTP) to synchronise data and results.

UCA10-1.2 Incomplete/ invalid data makes wrong data pre-process.

- Common time(NTP) to synchronise data and results.

UCA10-1.3 Incomplete/ invalid setting of the hyper-parameter.

- Common time(NTP) to synchronise data and results.

UCA10-1.4 Model suffered perturbed.

- Situational awareness.

UCA10-1.5 Incomplete/ invalid validation and verification.

- Sanity check.

UCA10-2.1 Wrong hyperparameter setting and model design.

- Sanity check for model architecture.
- Consistency check for the value ranges. of settings

UCA10-2.2 Data with wrong labels.

- Sanity check for the data label.

UCA10-2.3 Data was perturbed by external attackers.

- Situational awareness.

UCA10-2.4 Model suffered perturbed.

- Situational awareness.

UCA10-2.5 Incomplete/ invalid testing.

- Sanity check.

UCA10-2.6 Convolutional layer training not well.

- Retraining data.

UCA10-2.7 Non-max suppression layer selection is unreasonable.

- Setting a validated overlapping threshold (e.g., 0.5 typically).

UCA11.1 No command from local path planning component.

- Monitor systems should be used in normal situations.

UCA11.2 Kinematic model response delay.

- Monitor systems should be used in normal situations.

UCA11.3 Key command occurring too late.

- Monitor systems should be used normal situations.

UCA11.4 Kinematic model applied time too long.

- Monitor systems should be used normal situations.

UCA12.1 No command from Kinematic model to actuation system.

- Monitor systems should be used normal situations.

UCA12.2 Actuation system response delay.

- Monitor systems should be used normal situations.
- Sensor need to be more robust.

UCA12.3 Key command occurring too late.

- Monitor systems should be used normal situations.

UCA12.4 Actuation system applied time too long.

- Monitor systems should be used normal situations.
- Sensor need to be more robust.

UCA13.1 AUV management system do not passing command to the steering/Power/brake unit.

- Monitor systems should be used normal situations.

UCA13.2 AUV management system do not passing command to the monitor/measurement unit.

- Monitor systems should be used normal situations.

UCA13.3 Rotation/Position units do not send command to hardware.

- Monitor systems should be used normal situations.

UCA13.4 Rotation/Position units do not send feedback to the monitor.

- Monitor systems should be used normal situations.

UCA13.5 Each unit/monitor response delay.

- Monitor systems should be used normal situations.
- Sensor need to be more robust.

UCA13.6 Key command occurring too late.

- Monitor systems should be used normal situations.

UCA13.7 AUV condition monitor/ motor applied time too long.

- Monitor systems should be used normal situations.
- Sensor need to be more robust.

UCA14.1 No feedback to world or other components

- Monitor systems should be used normal situations.
- Sensor need to be more robust.

UCA14.2 Sent information is not timely to other components.

- Monitor systems should be used normal situations.
- Sensor need to be more robust.

UCa14.3 Feedback occurring too late.

- Monitor systems should be used normal situations.
- Sensor need to be more robust.

UCA14.4 Feedback information is incomplete.

- Monitor systems should be used normal situations.
- Sensor need to be more robust.