Introduction of VisualPro SA STPA and its application to VCU System

2023. 5

VWAY Co., Ltd.

Think Safety First

「 Contents 」

SW Safety Technologies
Global Leader

「 Contents 」

SW Safety Technologies
Global Leader

Introduction

VWAY?

Product and Services company, Specializing in Safety and Cybersecurity

Consulting for International Standards	Safety Management & Analysis SW	Provide Education of SW Safety Technology

Functional Safety and SW Safety Standard Model

- IEC 61508
- ISO 26262 (Automotive)
- ISO 21434 (Cybersecurity)
- IEC 62304 (Medical)
- IEC 61513 (Nuclear)
- IEC 62279, EN 50126(Railway)
- DO-178C(Aerospace)
- ISO 13482 (Robot)
- CMMI, ASPICE, SP

ALM Software, Functional & Security Safety Software

- Application Lifecycle Management
  - Establish a Safety Plan
  - Safety Traceability Management
- Safety Analysis SW
  - FMEA, FTA, STPA Safety Analysis
  - Based on AI (Automation)
- Cybersecurity Suite
  - TARA
  - SBOM & Audit Management

VisualPro SA With AI

Customer Customized Training Support

- Management of Safety Project
- Safety Analysis methods
- Education of Cyber Security
- Automotive Functional Safety Engineering Qualification Course (FSCE-FL)
- Education of SW Safety Experts
- Education of AI Safety

VWAY CAMPUS

Introduction

VWAY Activities for STPA

Presentation about STPA application in Korea
On Asia STAMP Workshop in Japan

Presentation about STPA and FTA
On ESWC(Europe Stamp Workshop Conference)

Presentation about Ensuring safety on VCU System
In ISO 26262 & SOTIF Conference 2023

Sponsorship on HIS(High Integrity Software)

Presentation about Autonomous Driving and STPA
on Korea Auto Industry & Global TransporTech Show

Presentation about Ensuring safety with STPA
on ISO 26262 & SOTIF Conference

Introduction

VisualPro SA STPA Customers

HYUNDAI MOTOR GROUP

KAERI Korea Atomic Energy Research Institute

KIAPI 지능형자동차부품진흥원 Korea Intelligent Automotive Parts Promotion Institute

OMRON

ktl 한국산업기술시험원 Korea Testing Laboratory

SCASD CONSULTING(USA)

Introduction

STPA Consulting Customers

HYUNDAI MOTOR GROUP

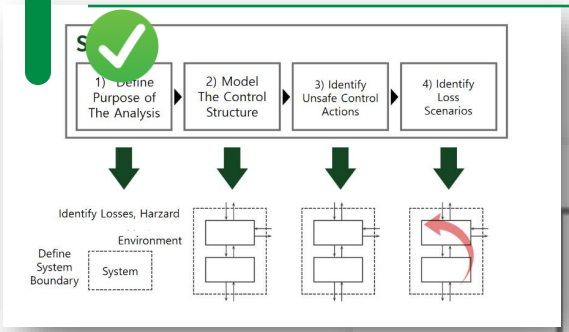
KARI 한국항공우주연구원 Korea Aerospace Research Institute

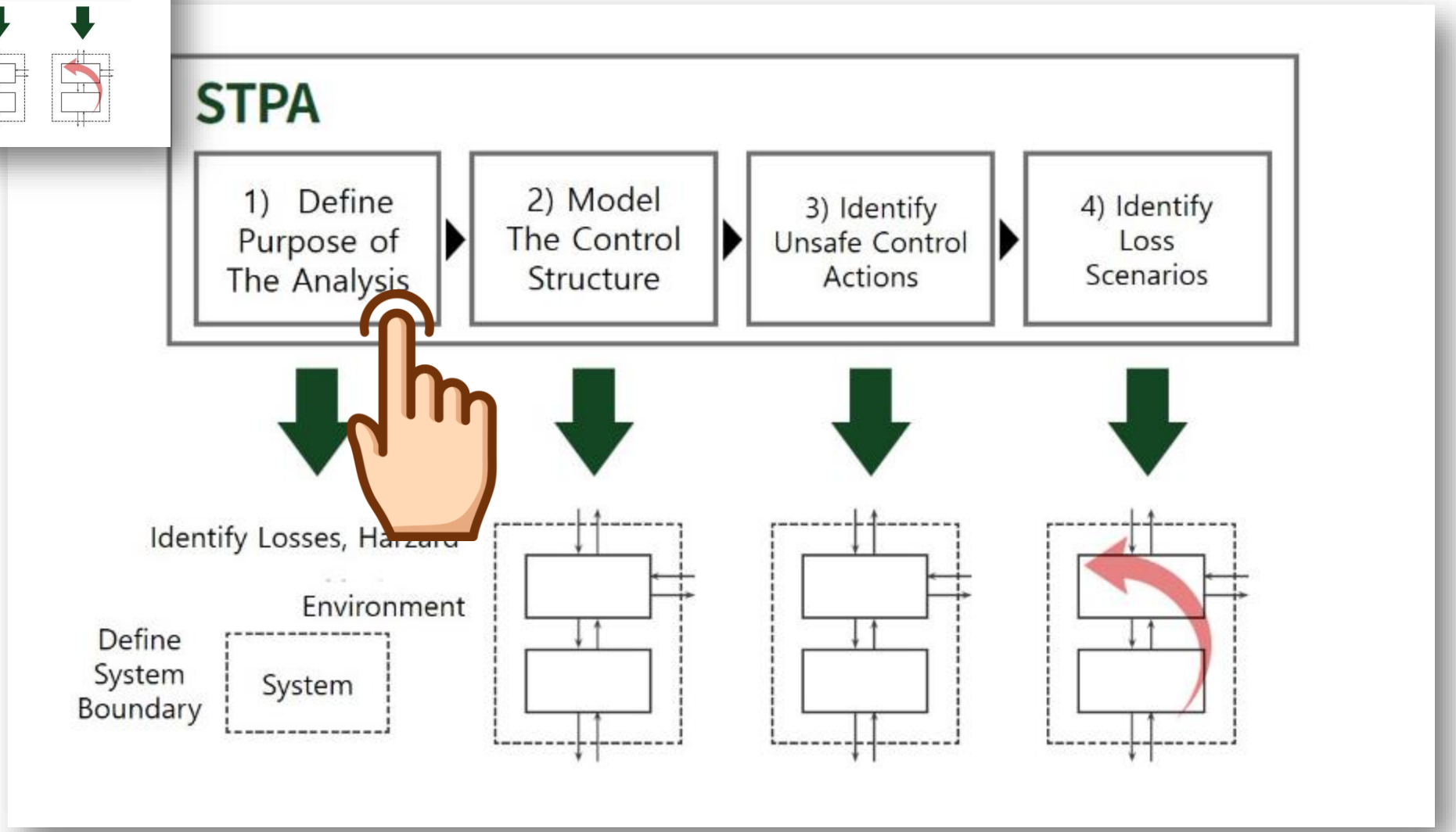
Universität Stuttgart

「 Contents 」

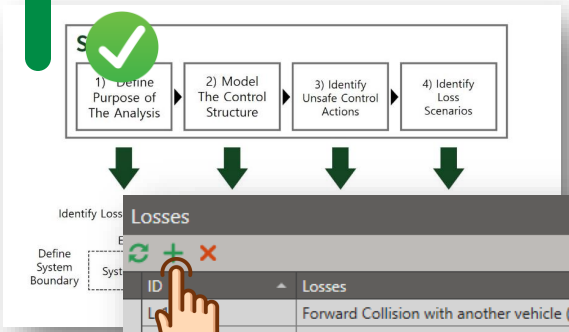
SW Safety Technologies
Global Leader

STPA on VCU System





STPA on VCU System



Losses

ID	Losses	Creator	Creation Date	Modified Person	Modified Date
L-	Forward Collision with another vehicle (Driver impairment/death is incurred or vehicle damage is resulted)	홍길동	2022-09-03 15:44	James	2022-12-14 17:23
L-	Backward Collision with another vehicle (Driver impairment/death is incurred or vehicle damage is resulted)	홍길동	2022-09-03 15:44	James	2022-12-14 17:24
L-3	Side Collision with another vehicle (Driver impairment/death is incurred or vehicle damage is resulted)	홍길동	2022-09-03 15:47	James	2022-12-14 17:24
L-4	Forward Collision with an object (Driver injury/death is resulted or object wreck or environmental pollution is caused)	홍길동	2022-09-03 15:52	James	2022-10-21 09:25
L-5	Backward Collision with an object (Driver injury/death is resulted or object wreck or environmental pollution is caused)	홍길동	2022-09-03 15:52	James	2022-10-21 09:26
L-6	Side Collision with an object (Driver injury/death is resulted or object wreck or environmental pollution is caused)	홍길동	2022-09-03 15:52	James	2022-10-21 09:26

Common Shortcut Menu

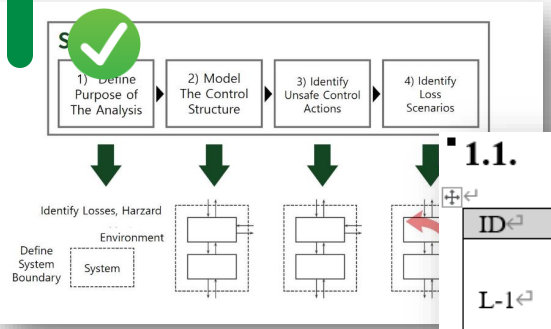
Refresh	ALT+R
Add row	ALT+A
Add child row	ALT+SHIFT+A
Delete row	ALT+D
Duplicate row	ALT+V

Losses Detail

ID: L-5

Detail:
A vehicle equipped with cVCU may get involved in a backward collision accident with an object.
'Object' here is defined as all identifiables except vehicles such as road objects, building, human life, animal, or stationary surroundings.
Driver injury or even death can be resulted from this collision as well as object wreck or environmental pollution.

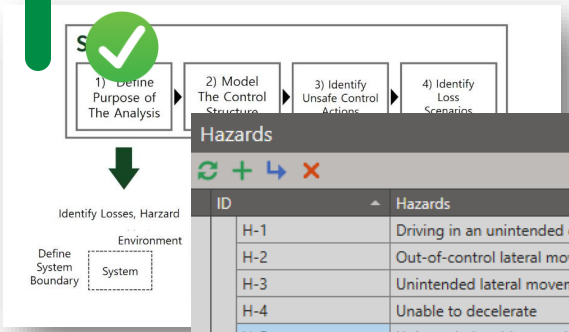
STPA on VCU System



1.1. VCU System Losses

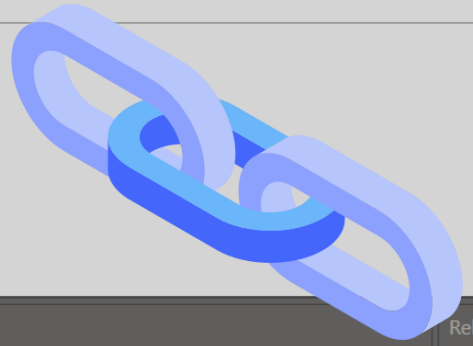
ID	Losses	Detail	Relationship
L-1	Forward Collision with another vehicle (Driver impairment/death is incurred or vehicle damage is resulted)	A vehicle equipped with cVCU may get involved in a forward collision accident. Driver injury or even death is expected or vehicle damage could be caused to both vehicles.	H-1, H-4, H-5
L-2	Backward Collision with another vehicle (Driver impairment/death is incurred or vehicle damage is resulted)	A vehicle equipped with cVCU may get involved in a backward collision accident. Driver injury or even death is expected or vehicle damage could be caused to both vehicles.	H-1, H-6, H-7, H-8
L-3	Side Collision with another vehicle (Driver impairment/death is incurred or vehicle damage is resulted)	A vehicle equipped with cVCU may get involved in a side collision accident. Driver injury or even death is expected or vehicle damage could be caused to both vehicles.	H-2, H-3, H-5, H-8
L-4	Forward Collision with an object (Driver injury/death is resulted or object wreck or environmental pollution is caused)	A vehicle equipped with cVCU may get involved in a forward collision accident with an object. 'Object' here is defined as all identifiable except vehicles such as road objects, building, human life, animal, or stationary surroundings. Driver injury or even death can be resulted from this collision as well as object wreck or environmental pollution.	H-1, H-4, H-5
L-5	Backward Collision with an object (Driver injury/death is resulted or object wreck or environmental pollution is caused)	A vehicle equipped with cVCU may get involved in a backward collision accident with an object. 'Object' here is defined as all identifiable except vehicles such as road objects, building, human life, animal, or stationary surroundings. Driver injury or even death can be resulted from this collision as well as object wreck or environmental pollution.	H-1
L-6	Side Collision with an object (Driver injury/death is resulted or object wreck or environmental pollution is caused)	A vehicle equipped with cVCU may get involved in a side collision accident with an object. 'Object' here is defined as all identifiable except vehicles such as road objects, building, human life, animal, or stationary surroundings. Driver injury or even death can be resulted from this collision as well as object wreck or environmental pollution.	H-2, H-3, H-8

STPA on VCU System



Hazards

ID	Hazards	Creator	Creation Date	Modified Person	Modified Date
H-1	Driving in an unintended direction	홍길동	2022-09-03 16:02	James	2022-12-14 17:33
H-2	Out-of-control lateral movement	홍길동	2022-09-03 16:02	James	2022-12-14 17:27
H-3	Unintended lateral movement	홍길동	2022-09-03 16:02	James	2022-12-14 17:28
H-4	Unable to decelerate	홍길동	2022-09-03 16:02	James	2022-12-14 17:29
H-5	Unintended sudden acceleration	홍길동	2022-09-03 16:02	James	2022-12-14 17:29
H-6	Unintended sudden deceleration	홍길동	2022-09-03 16:02	James	2022-12-14 17:30
H-7	Unable to accelerate	홍길동	2022-09-03 16:02	James	2022-12-14 17:32
H-8	Unintended sudden stalling	홍길동	2022-09-03 16:02	James	2022-12-14 17:32



Hazards Detail

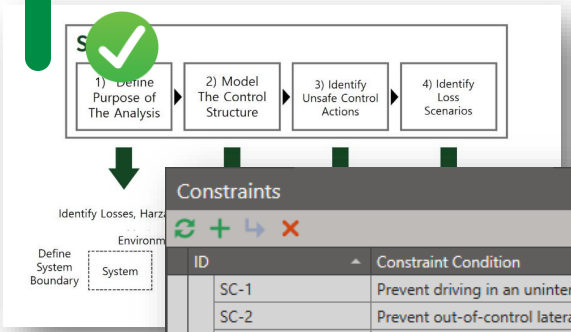
ID: H-5

Detail: The vehicle makes a sudden, unintended acceleration at the speed of over 20 km per hour while at a stop or on normal driving.

Relationship

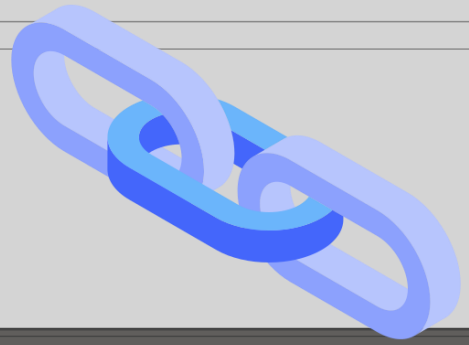
	ID	Losses
☑	L-1	Forward Collision with another vehicle (Driver impairment/death is incurred or vehicle damag...
☐	L-2	Backward Collision with another vehicle (Driver impairment/death is incurred or vehicle dama...
☑	L-3	Side Collision with another vehicle (Driver impairment/death is incurred or vehicle damage is...
☑	L-4	Forward Collision with an object (Driver injury/death is resulted or object wreck or environme...
☐	L-5	Backward Collision with an object (Driver injury/death is resulted or object wreck or environm...
☐	L-6	Side Collision with an object (Driver injury/death is resulted or object wreck or environmental...

STPA on VCU System



Constraints

ID	Constraint Condition	Creator	Creation Date	Modified Person	Modified Date
SC-1	Prevent driving in an unintended direction	홍길동	2022-09-03 16:10	James	2022-12-14 17:36
SC-2	Prevent out-of-control lateral movement	홍길동	2022-09-03 16:10	James	2022-12-14 17:36
SC-3	Prevent unintended lateral movement	홍길동	2022-09-03 16:10	James	2022-12-14 17:36
SC-4	Prevent being unable to decelerate	홍길동	2022-09-03 16:11	James	2022-12-14 17:36
SC-5	Prevent unintended sudden acceleration	홍길동	2022-09-03 16:11	James	2022-12-14 17:36
SC-6	Prevent unintended sudden deceleration	홍길동	2022-09-03 16:11	James	2022-12-14 17:36
SC-7	Prevent being unable to accelerate	홍길동	2022-09-03 16:11	James	2022-12-14 17:36
SC-8	Prevent unintended sudden stalling	홍길동	2022-09-03 16:11	James	2022-12-14 17:37



Constraints Detail

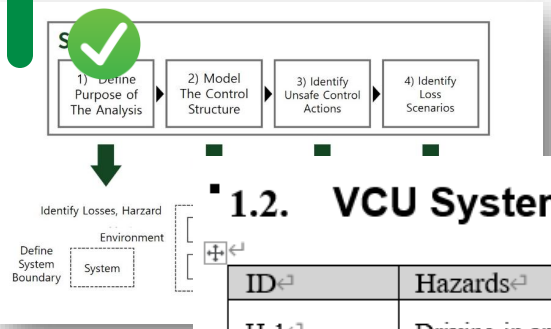
ID

Detail

Relationship

ID	Hazards
H-1	Driving in an unintended direction
H-2	Out-of-control lateral movement
H-3	Unintended lateral movement
H-4	Unable to decelerate
H-5	Unintended sudden acceleration
H-6	Unintended sudden deceleration
H-7	Unable to accelerate
H-8	Unintended sudden stalling

STPA on VCU System



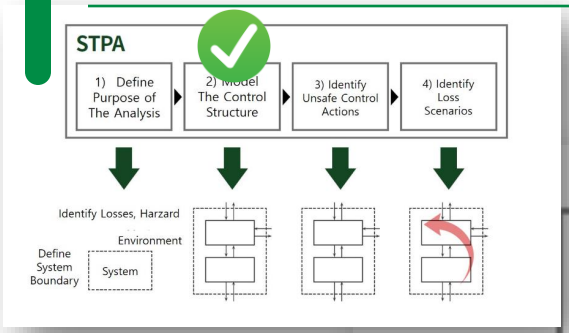
1.2. VCU System Hazards

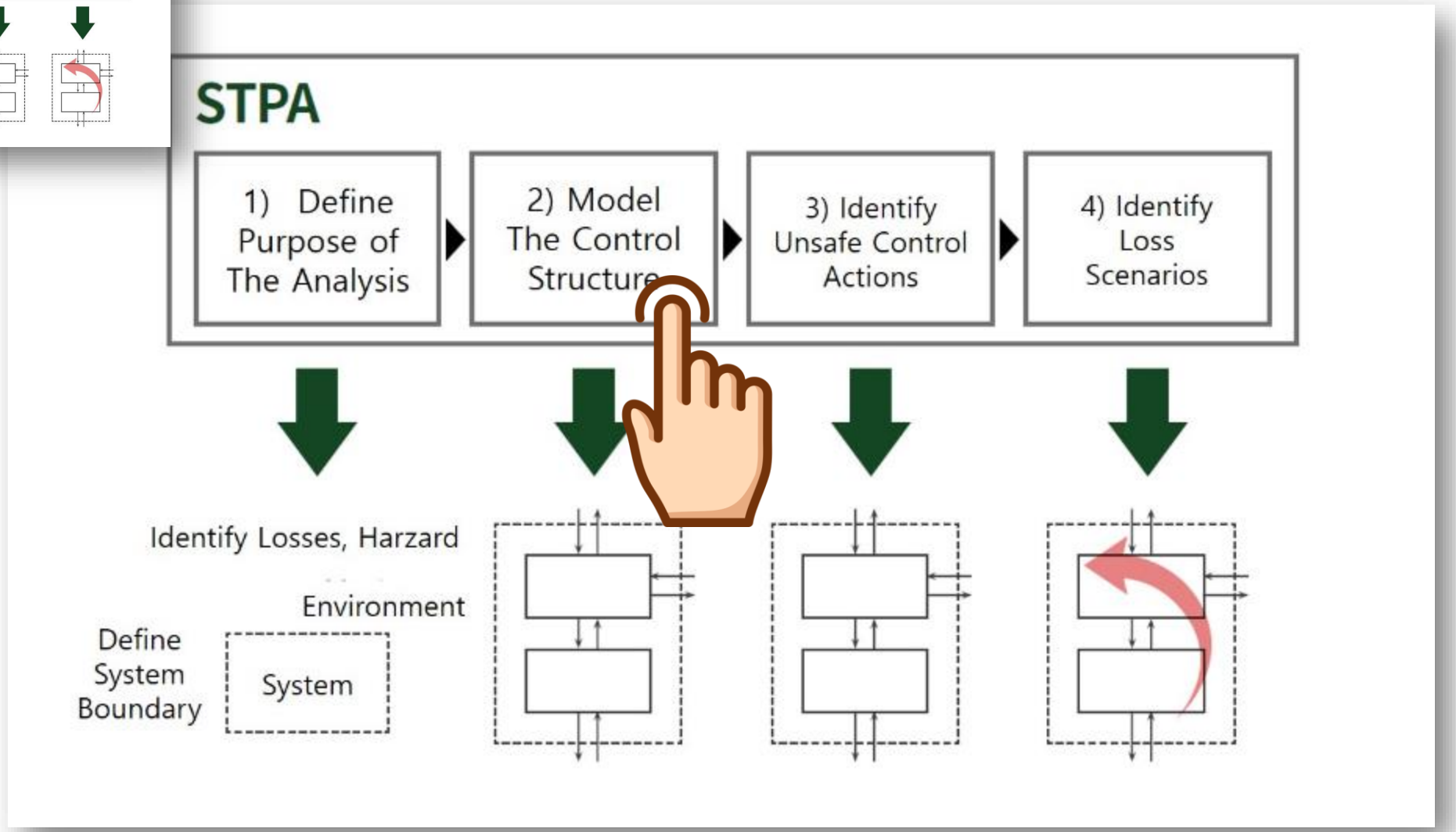
ID	Hazards	Detail	Relationship
H-1	Driving in an unintended direction	A faulty cVCU computer command makes the vehicle go backwards when it's supposed to go forward, or vice versa.	L-1, L-2, L-4, L-5
H-2	Out-of-control lateral movement	cVCU controller cannot perform left and right movement control.	L-3, L-6
H-3	Unintended lateral movement	A faulty cVCU computer command triggers a sudden left or right turn. For instance, it wrongly orders a left turn instead of right, or vise versa.	L-3, L-6
H-4	Unable to decelerate	Deceleration is not properly executed when head-on collision with another vehicle or objects ahead needs to be avoided.	L-1, L-4
H-5	Unintended sudden acceleration	The vehicle makes a sudden, unintended acceleration at the speed of over 20 km per hour while at a stop or on normal driving.	L-1, L-3, L-4
H-6	Unintended sudden deceleration	The vehicle makes a sudden, unintended deceleration at the speed of over 20 km per hour while on normal driving.	L-2
H-7	Unable to accelerate	Acceleration is not properly executable when needed at a complete stop or on normal driving.	L-2
H-8	Unintended sudden stalling	The vehicle makes a sudden stall while on drive, in the case of which no sideways control is provided or unintended deceleration is made.	L-2, L-3, L-6

1.3. VCU System Constraints

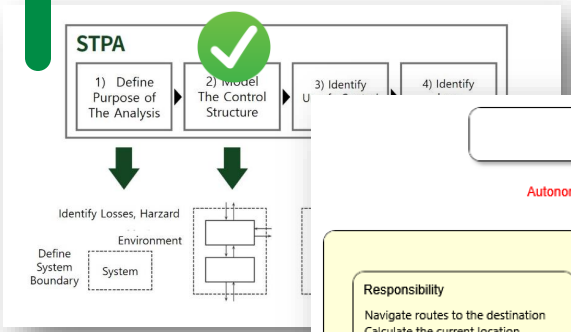
ID	Constraints	Detail	Relationship
SC-1	Prevent driving in an unintended direction	Hazards for driving in an unintended direction must be prevented.	H-1
SC-2	Prevent out-of-control lateral movement	Hazards for out-of-control lateral movement must be prevented.	H-2
SC-3	Prevent unintended lateral movement	Hazards for unintended lateral movement must be prevented.	H-3
SC-4	Prevent being unable to decelerate	Hazards for being unable to decelerate must be prevented.	H-4
SC-5	Prevent unintended sudden acceleration	Hazards for unintended sudden acceleration must be prevented.	H-5
SC-6	Prevent unintended sudden deceleration	Hazards for unintended sudden deceleration must be prevented.	H-6
SC-7	Prevent being unable to accelerate	Hazards for being unable to accelerate must be prevented.	H-7
SC-8	Prevent unintended sudden stalling	Hazards for unintended sudden stalling must be prevented.	H-8

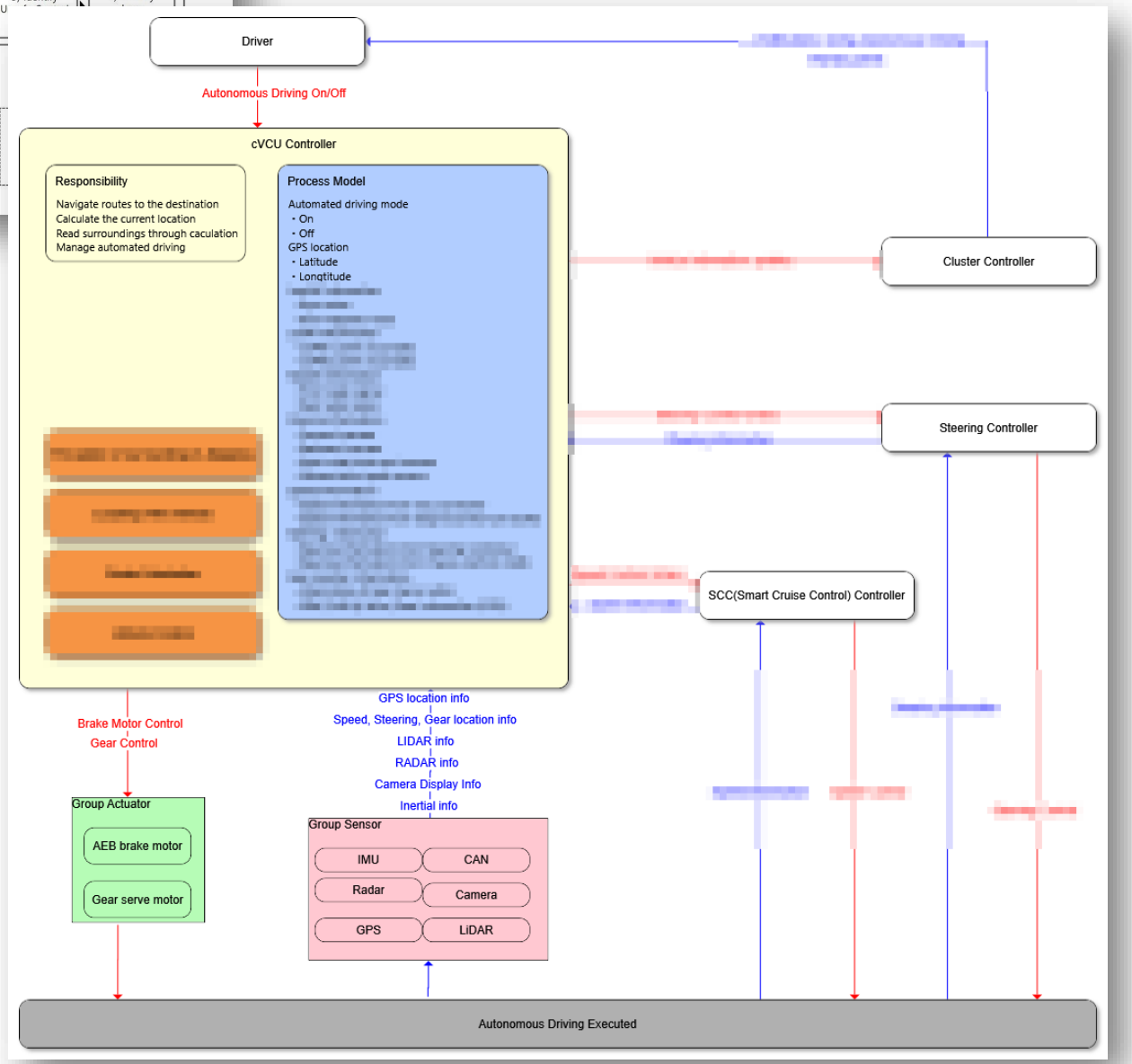
STPA on VCU System





STPA on VCU System

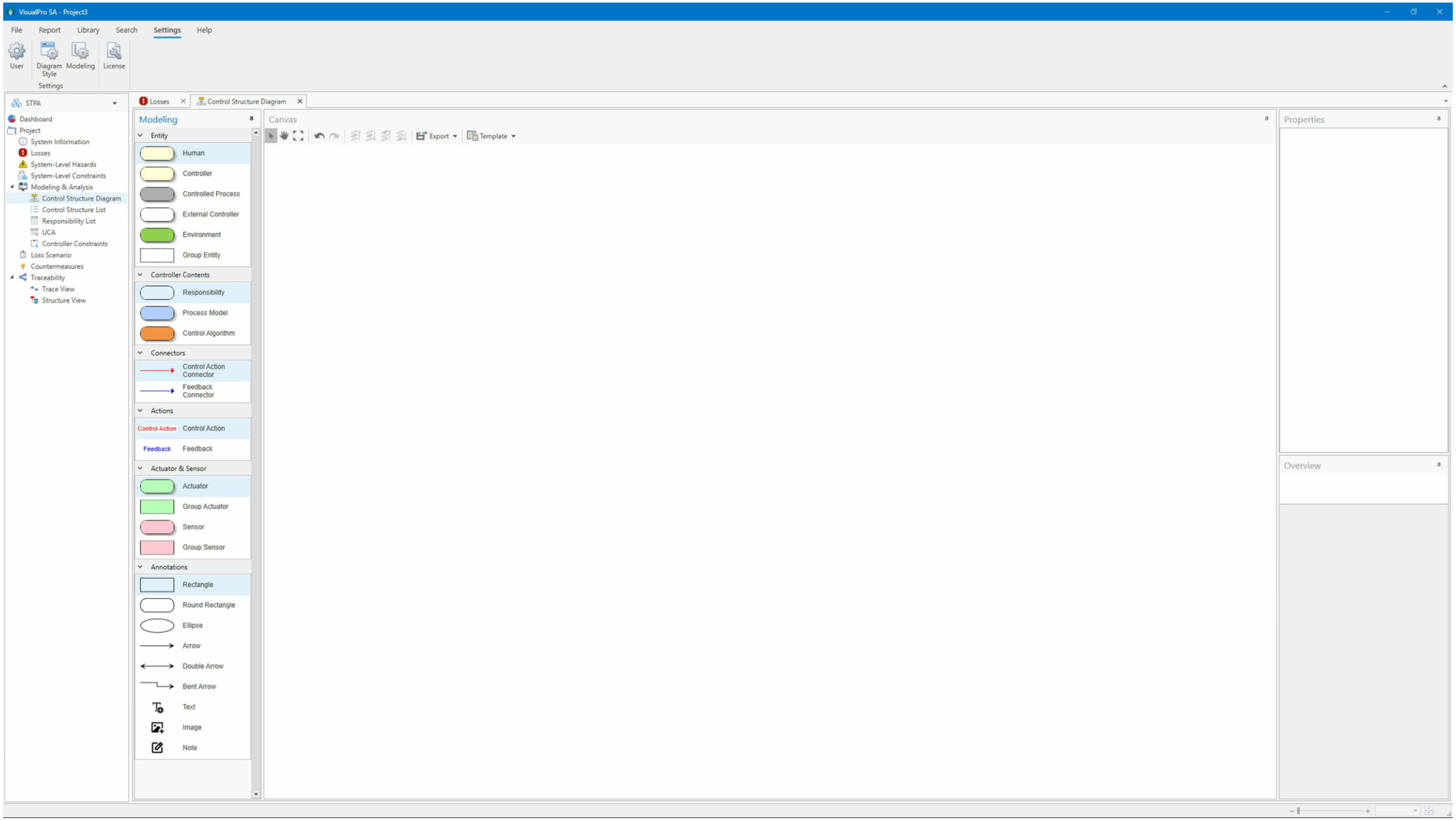




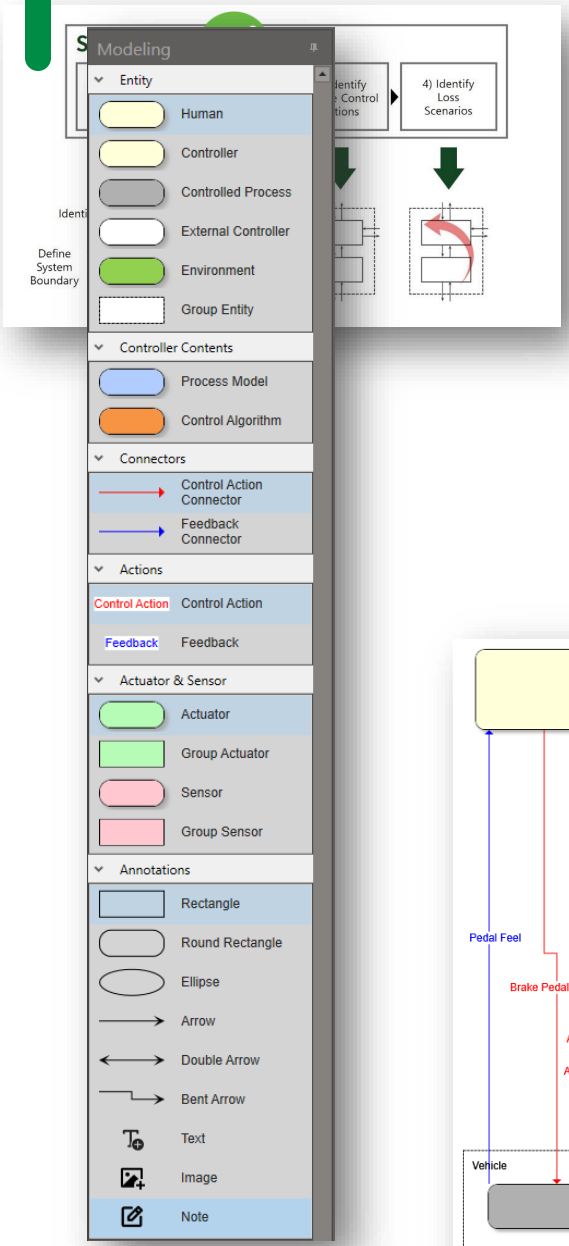
Control Action Connector → Feedback Connector

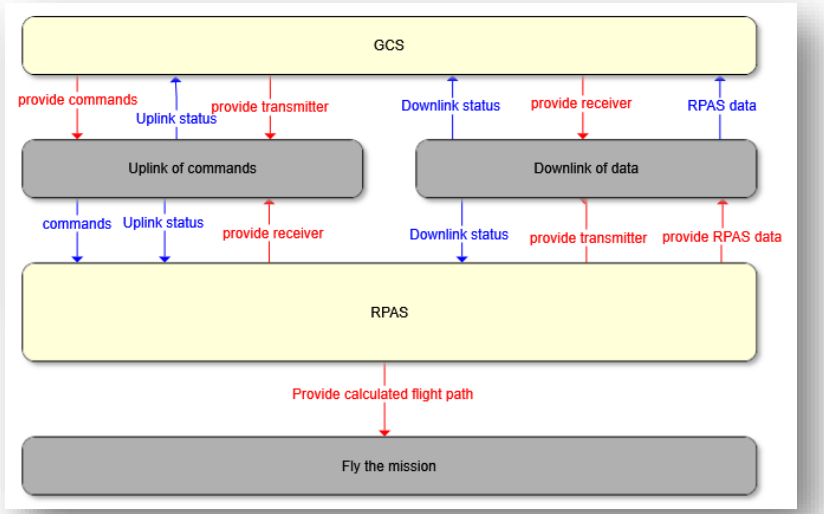
- VCU controlled by Driver
- VCU controls Steering, Cluster, SCC controller
- VCU controls Autonomous Driving with Brake Motor control and Gear Control
- VCU get the feedback from IMU, CAN, RADAR, Camera, GPS, Lidar
- It may look similar to the system architecture. However, STPA reconstructs the system's structure from a control perspective.

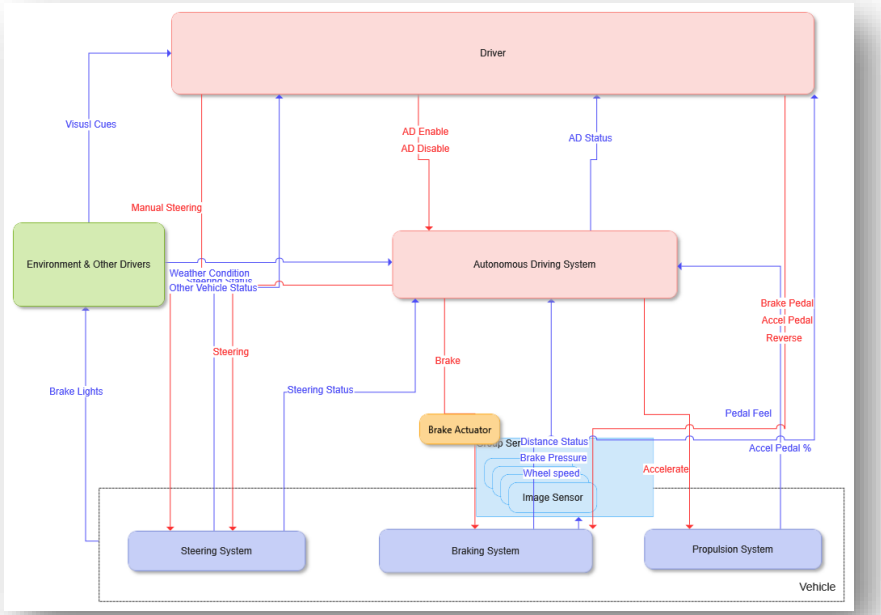
STPA on VCU System

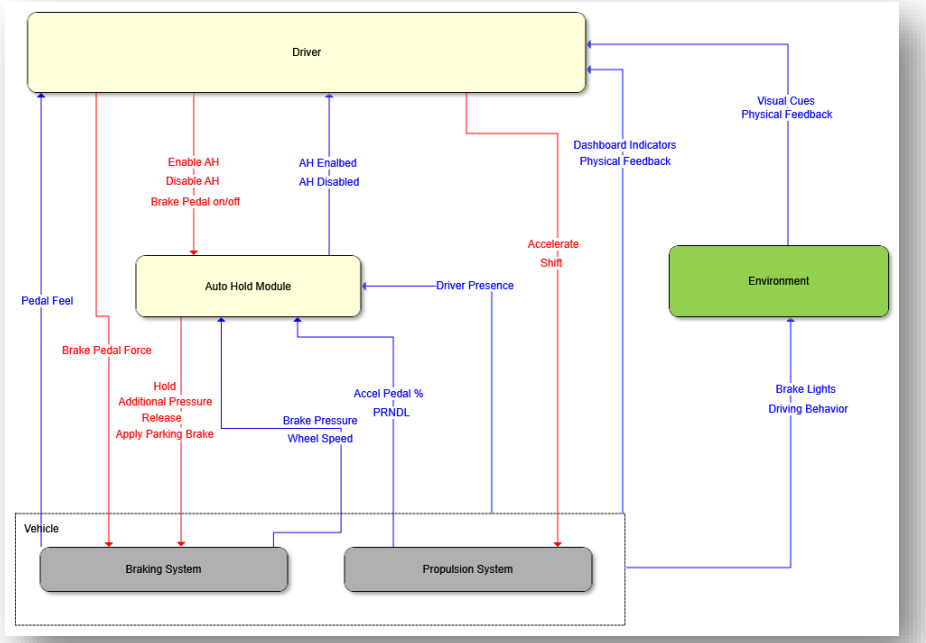


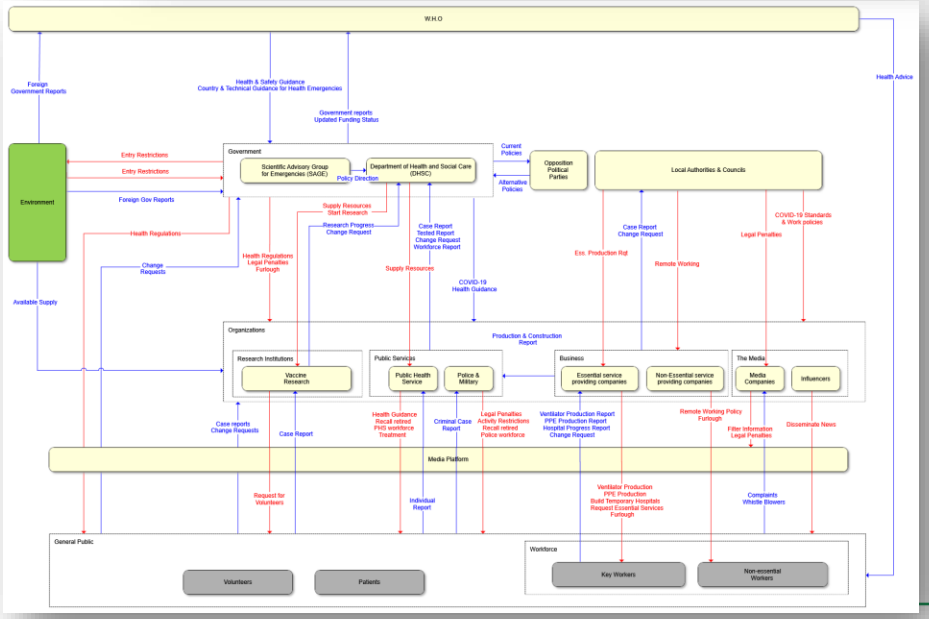
STPA on VCU System



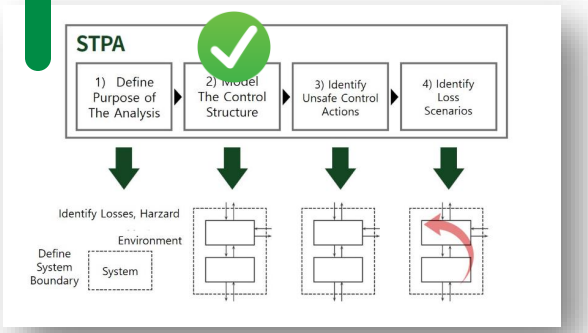


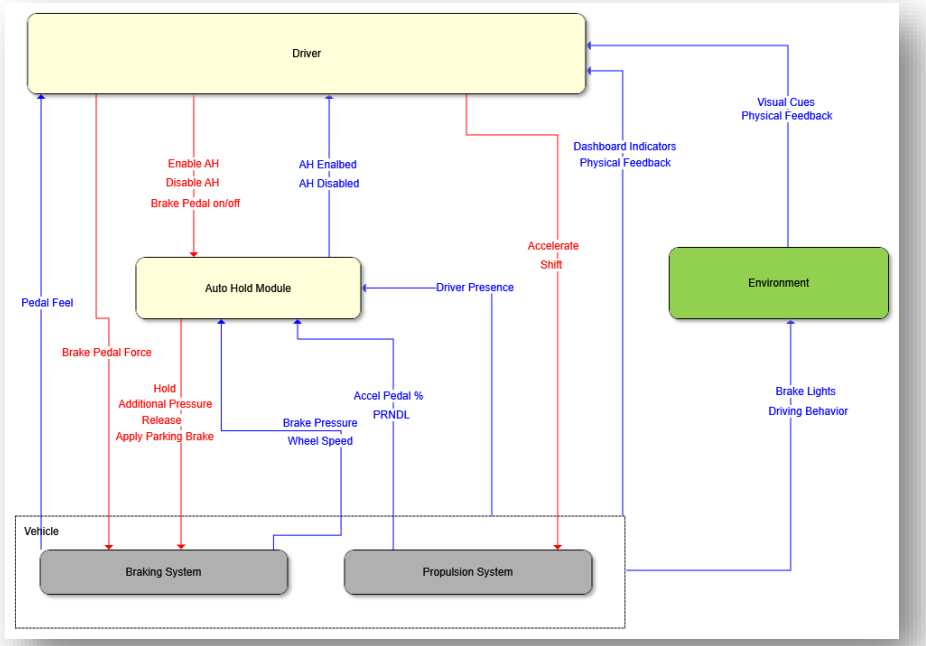


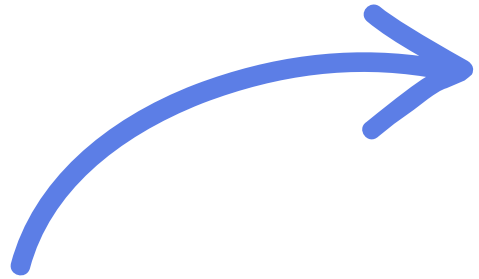




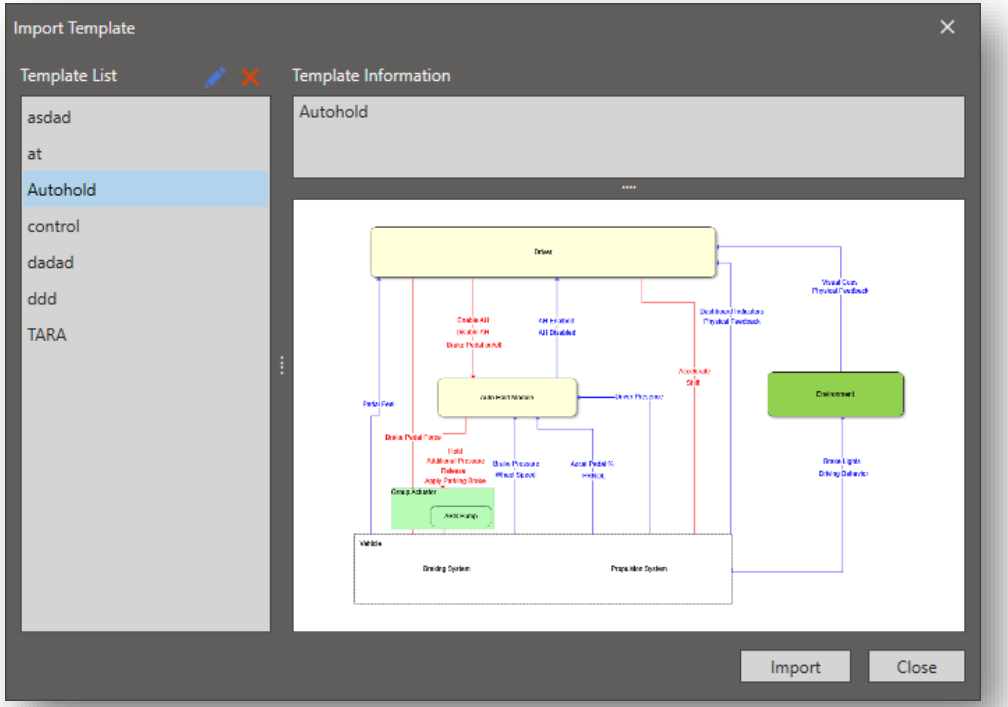
STPA on VCU System





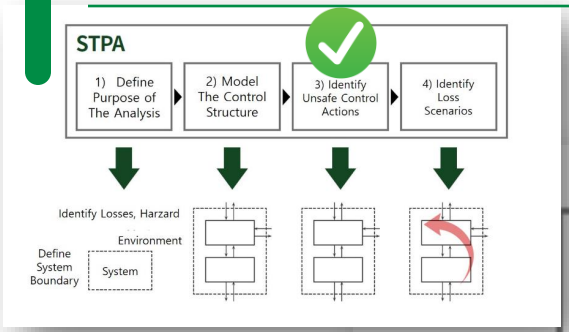


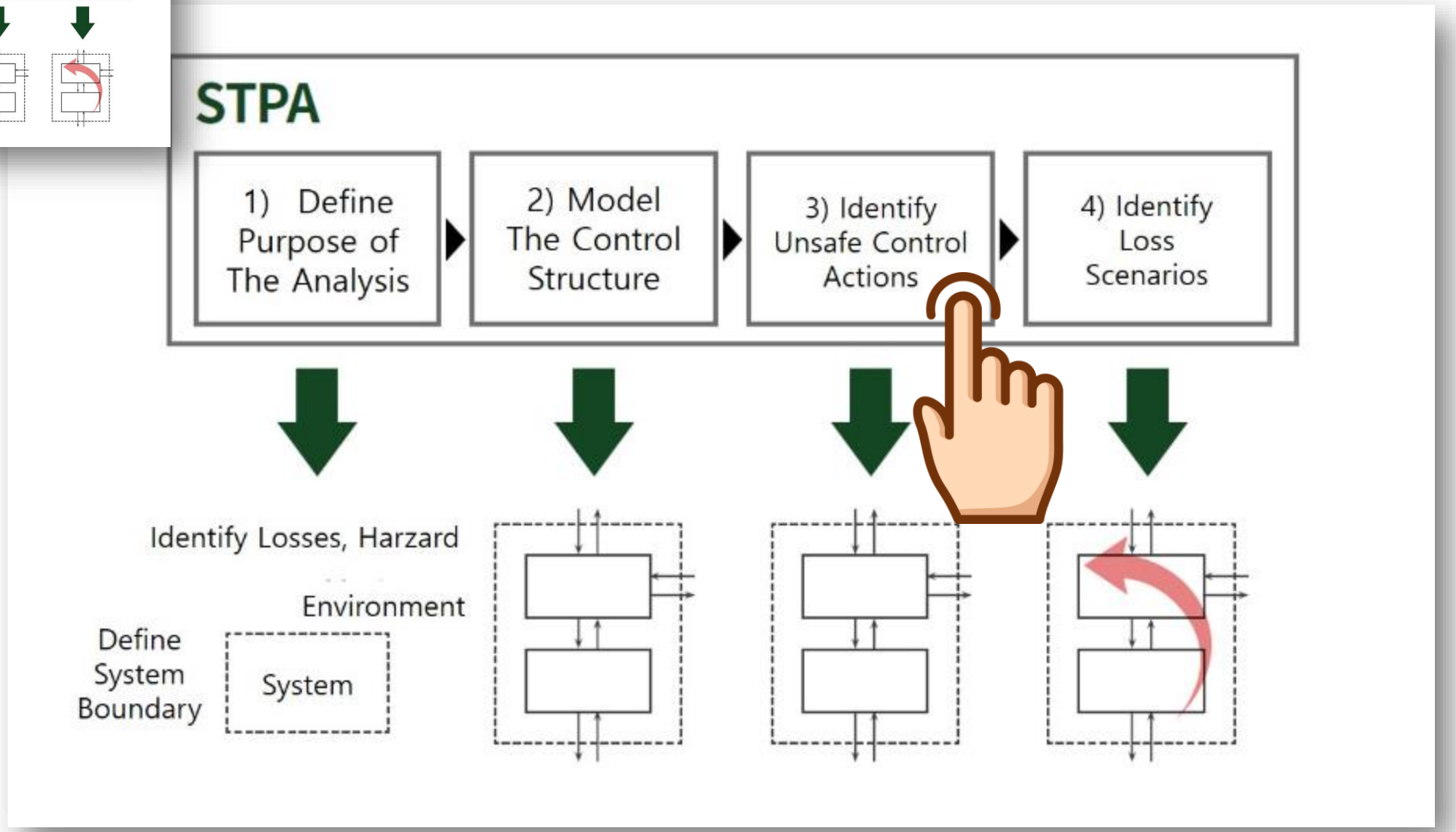
SVG
PNG



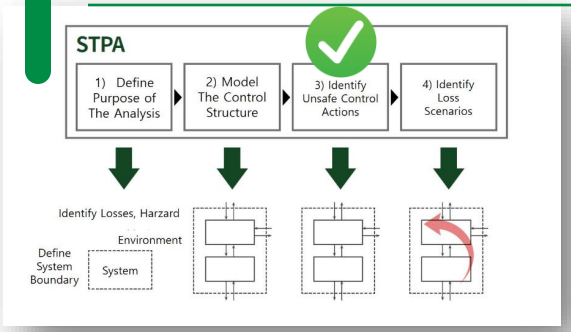
Reusable through template

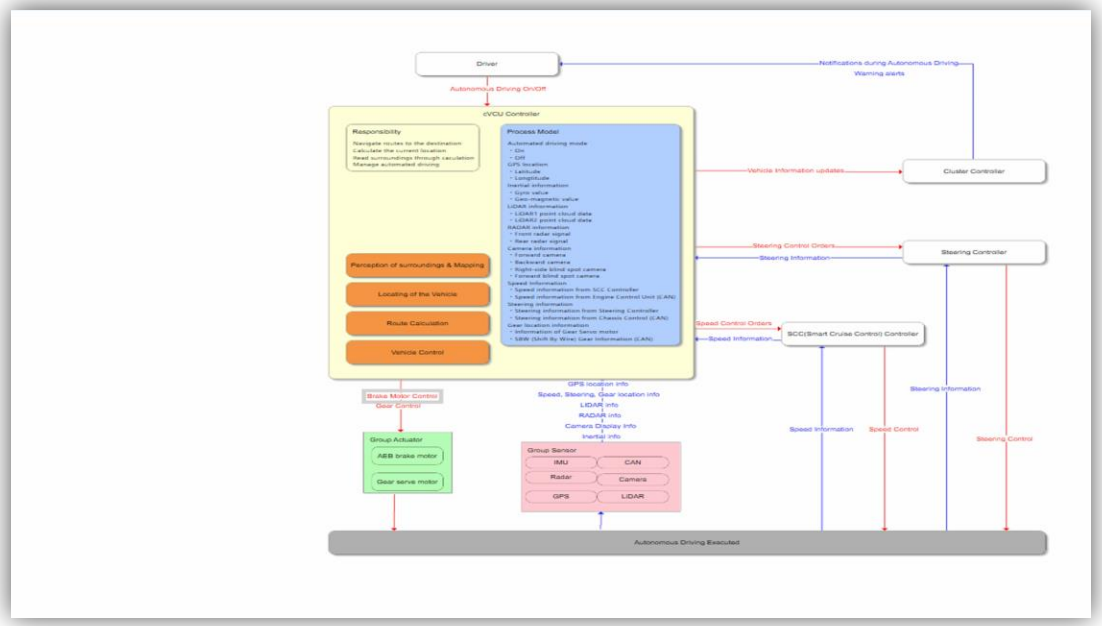
STPA on VCU System





STPA on VCU System





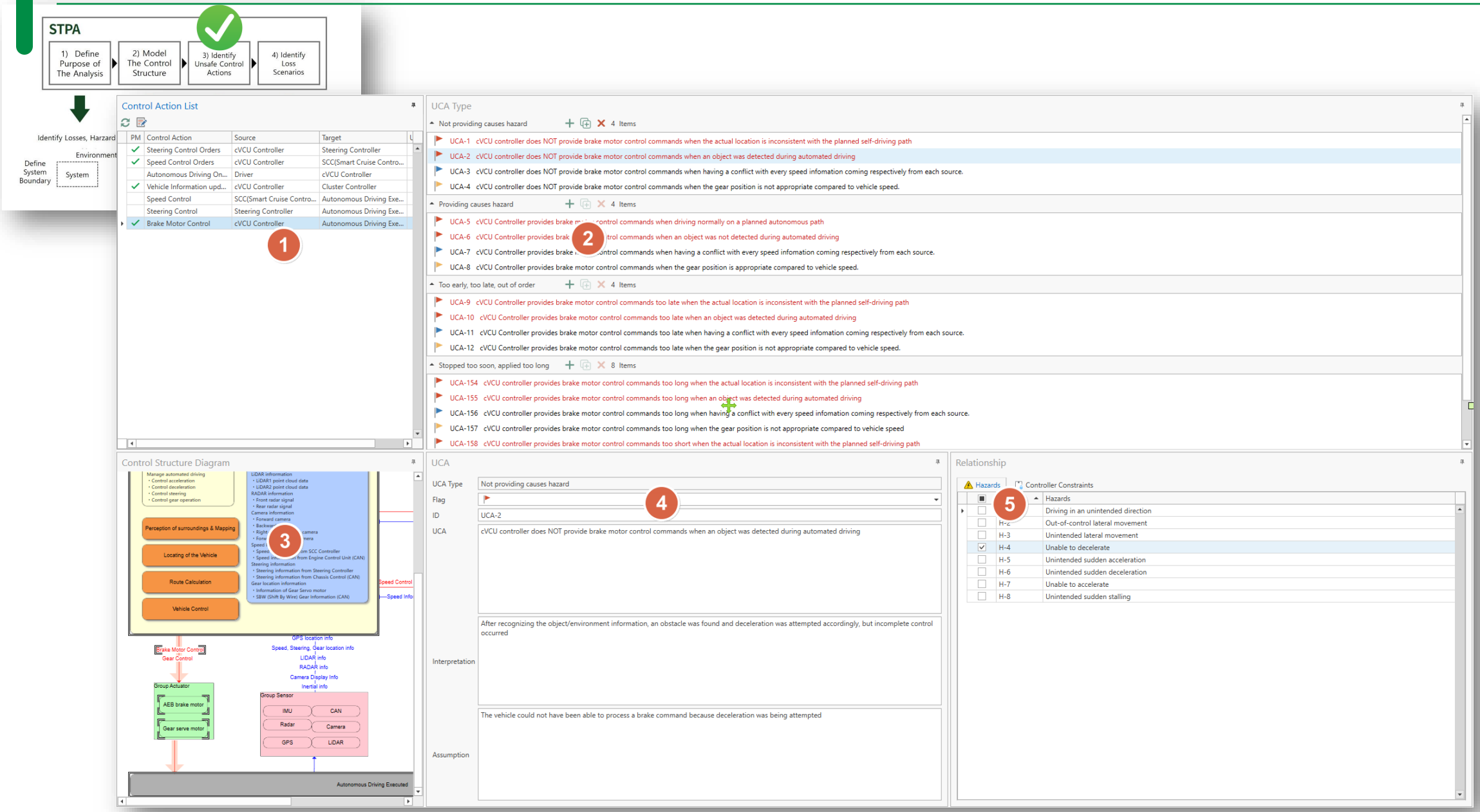
UCA = Unsafe Control Action

UCA has 4 types

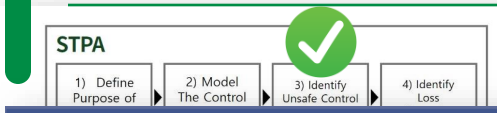
- Not providing causes hazard
- Providing causes hazard
- Too early, too late, out of order
- Stopped too soon, applied too long

Brake Motor Control

STPA on VCU System



STPA on VCU System



Control Action List

Brake Motor Control	cVCU Controller	Autonomous Driving Exe...	1

UCA Type

Not providing causes hazard — 4 Items

UCA-1 cVCU controller does NOT provide brake motor control commands when the actual location is inconsistent with the planned self-driving path

Providing causes hazard — 4 Items

UCA-5 cVCU Controller provides brake motor control commands when driving normally on a planned autonomous path

Too early, too late, out of order — 4 Items

UCA-9 cVCU Controller provides brake motor control commands too late when the actual location is inconsistent with the planned self-driving path

Stopped too soon, applied too long — 8 Items

UCA-154 cVCU controller provides brake motor control commands too long when the actual location is inconsistent with the planned self-driving path

UCA-155 cVCU controller provides brake motor control commands too long when an object was detected during automated driving

UCA-5 cVCU Controller provides brake motor control commands when driving normally on a planned autonomous path

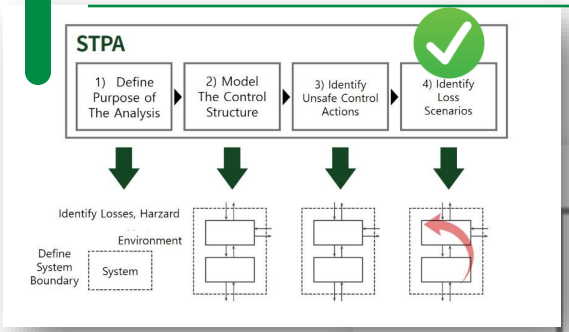
Relationship

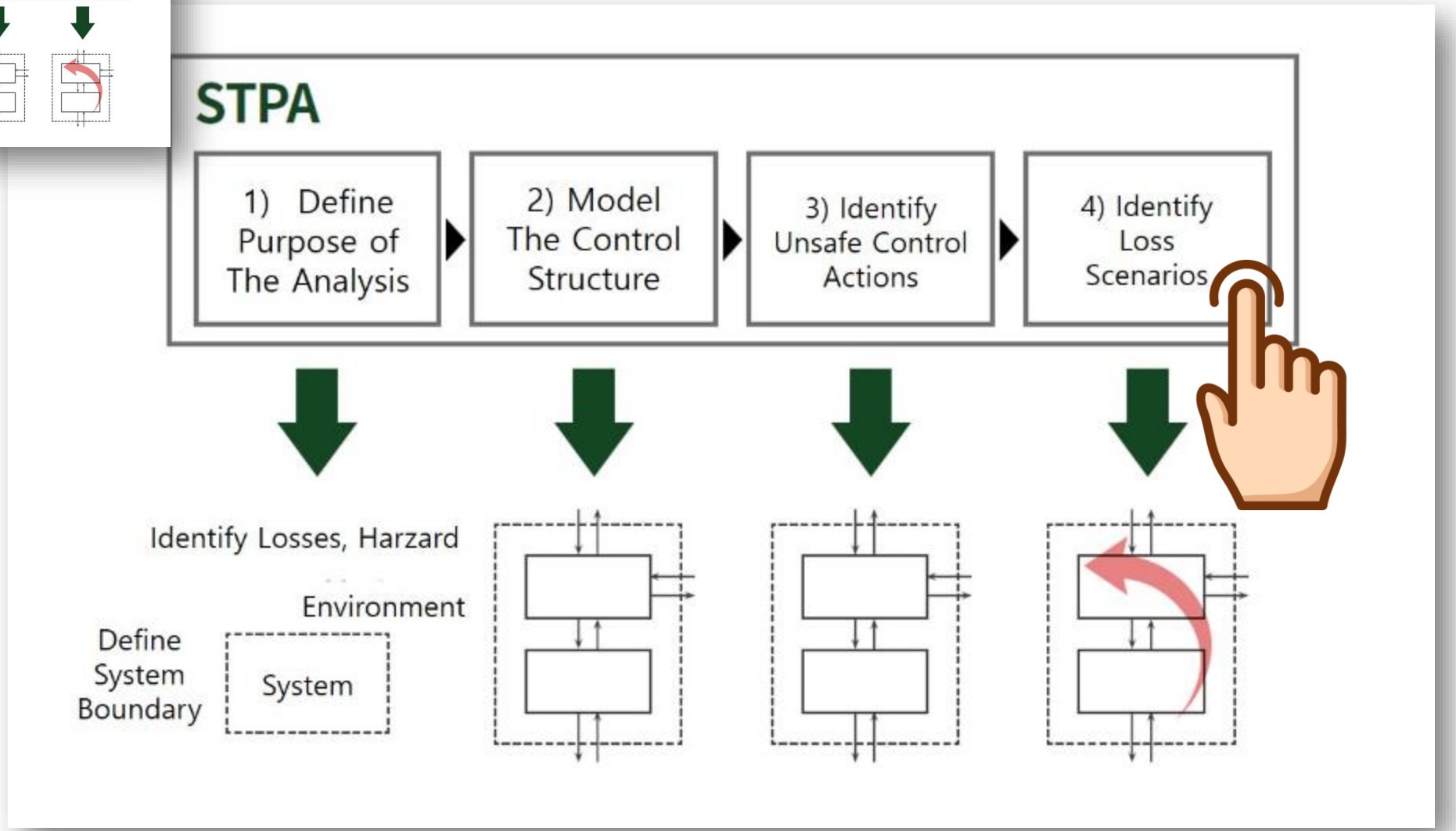
Hazards | Controller Constraints

ID	Hazards
H-1	Driving in an unintended direction
H-2	Out-of-control lateral movement
H-3	Unintended lateral movement
H-4	Unable to decelerate
H-5	Unintended sudden acceleration
H-6	Unintended sudden deceleration
H-7	Unable to accelerate
H-8	Unintended sudden stalling

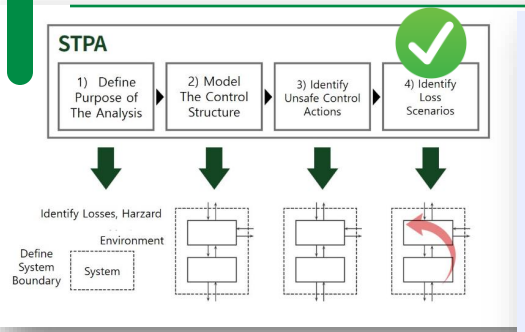
UCA has to be linked with Hazards

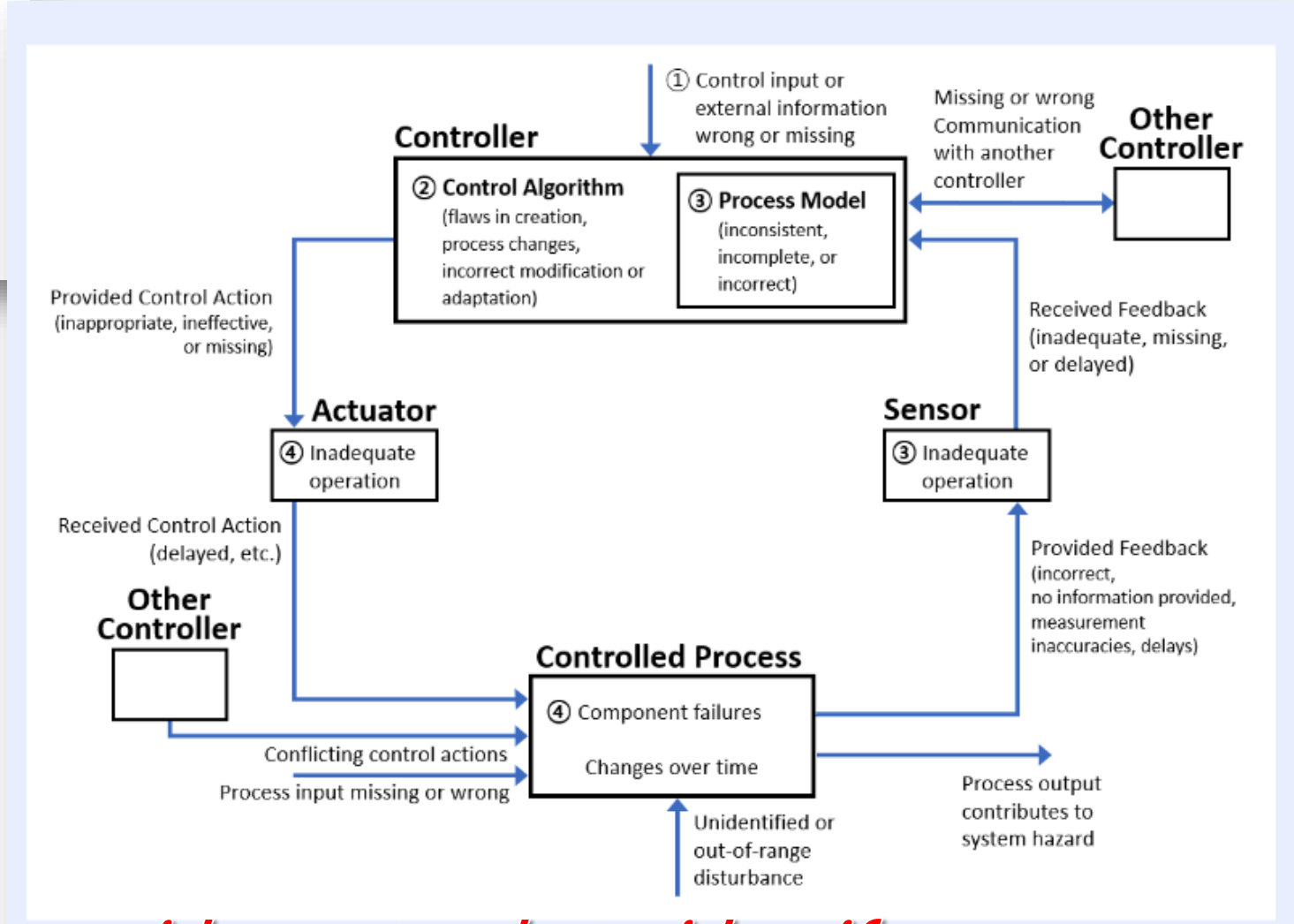
STPA on VCU System





STPA on VCU System

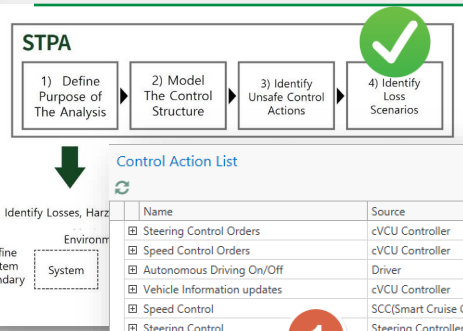




STPA can consider not only to identify component failures, but also control failures and non component failures, misuses.

An STPA Primer, 2013

STPA on VCU System



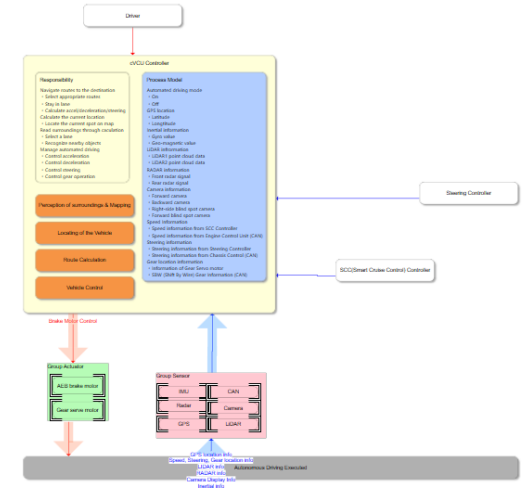
Control Action List

Name	Source	Target
Steering Control Orders	cVCU Controller	Steering Controller
Speed Control Orders	cVCU Controller	SCC(Smart Cruise Control) Controller
Autonomous Driving On/Off	Driver	cVCU Controller
Vehicle Information updates	cVCU Controller	Cluster Controller
Speed Control	SCC(Smart Cruise Control) Controller	Autonomous Driving Executed
Steering Control	Steering Controller	Autonomous Driving Executed
Brake Motor Control	cVCU Controller	Autonomous Driving Executed

Flag	ID	UCA
	UCA-1	19 cVCU controller does NOT provide brake motor control commands when the actual location is inconsistent with the planned self-driving path
	UCA-2	21 cVCU controller does NOT provide brake motor control commands when an object was detected during automated driving
	UCA-3	0 cVCU controller does NOT provide brake motor control commands when having a conflict with every speed infomation coming respectively from
	UCA-4	0 cVCU controller does NOT provide brake motor control commands when the gear position is not appropriate compared to vehicle speed.
	UCA-5	37 cVCU Controller provides brake motor control commands when driving normally on a planned autonomous path
	UCA-6	20 cVCU Controller provides brake motor control commands when an object was not detected during automated driving
	UCA-7	0 cVCU Controller provides brake motor control commands when having a conflict with every speed infomation coming respectively from each sou
	UCA-8	0 cVCU Controller provides brake motor control commands when the gear position is appropriate compared to vehicle speed.
	UCA-9	16 cVCU Controller provides brake motor control commands too late when the actual location is inconsistent with the planned self-driving path
	UCA-10	18 cVCU Controller provides brake motor control commands too late when an object was detected during automated driving
	UCA-11	0 cVCU Controller provides brake motor control commands too late when having a conflict with every speed infomation coming respectively from e
	UCA-12	0 cVCU Controller provides brake motor control commands too late when the gear position is not appropriate compared to vehicle speed.
	UCA-154	17 cVCU Controller provides brake motor control commands too long when the actual location is inconsistent with the planned self-driving path
	UCA-155	19 cVCU controller provides brake motor control commands too long when an object was detected during automated driving
	UCA-156	0 cVCU controller provides brake motor control commands too long when having a conflict with every speed infomation coming respectively from
	UCA-157	0 cVCU controller provides brake motor control commands too long when the gear position is not appropriate compared to vehicle speed
	UCA-158	17 cVCU controller provides brake motor control commands too short when the actual location is inconsistent with the planned self-driving path

Control Loop

Show Additional Considerations



Loss Scenario

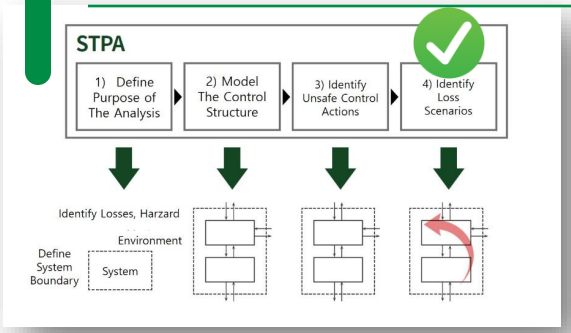
Scenarios with UCA : UCA-5 | Scenarios without UCA

Auto Creation of Loss Scenario

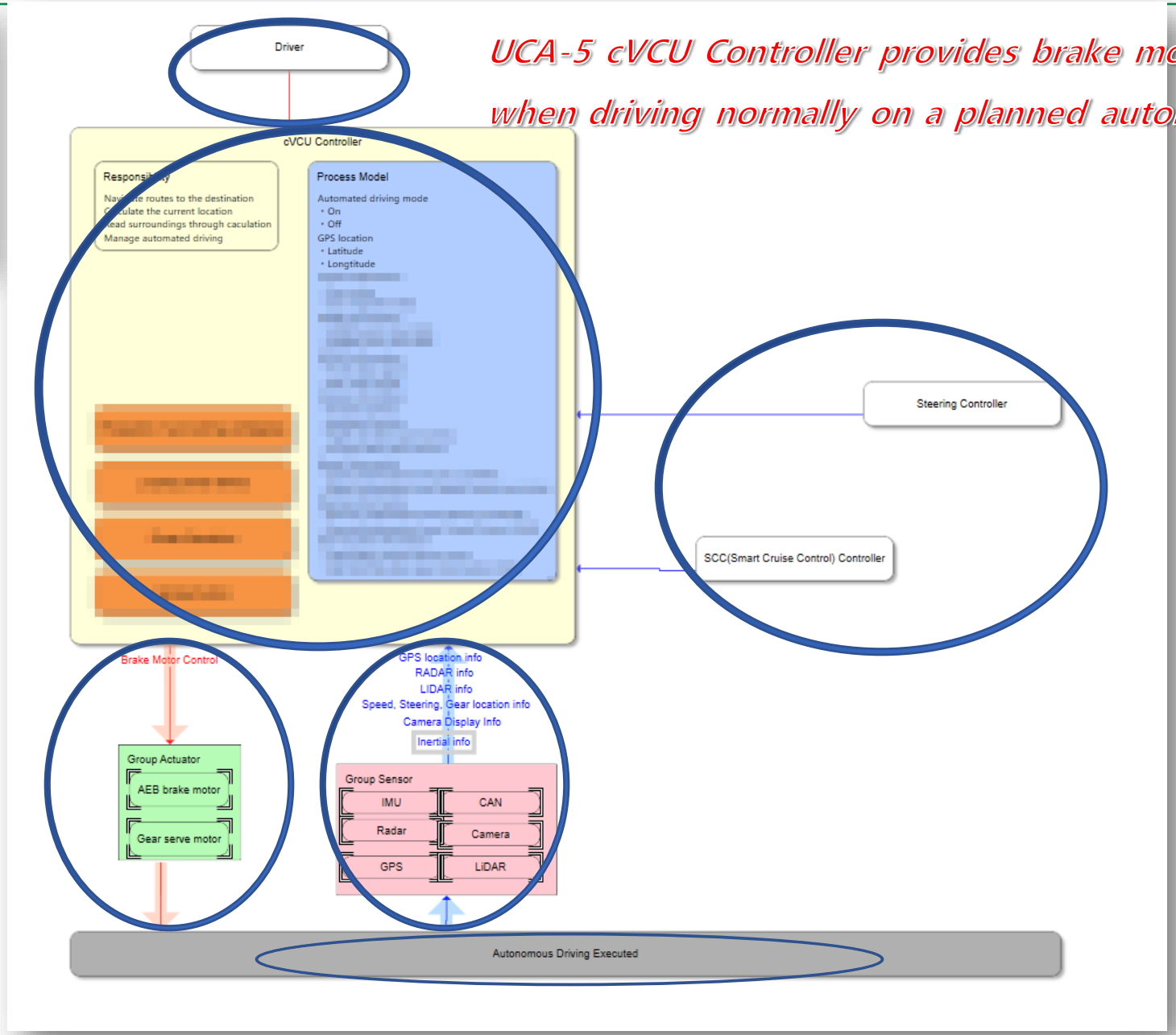
Guide Word Set :

ID	Flag	Entity	Guide Word	Loss Scenario	Creator	Creation Date	Modified P...	Modified Date
LS-21		cVCU Controller	Physical failure of the controller itself	cVCU Controller provides a brake motor control command due to a physical failure during planned autonomous driving	홍길동	2022-09-28 21:41	James	2022-12-21 09:37
LS-21-1		cVCU Controller	Physical failure of the controller itself	Microprocessor (μC) with low-reliability was used	홍길동	2022-09-28 21:41	James	2022-12-21 09:36
LS-22		cVCU Controller	Power failure	cVCU controller provides a brake motor control command due to a power failure while driving normally on the planned self-driving path	홍길동	2022-09-28 21:41	James	2022-12-21 09:37
LS-22-1		cVCU Controller	Power failure	Unstable power supply (high voltage, low voltage, etc.)	홍길동	2022-09-28 21:41	James	2022-12-21 09:37
LS-22-2		cVCU Controller	Power failure	Power regulator with low reliability was used	홍길동	2022-09-28 21:44	James	2022-12-21 09:37
LS-23		cVCU Controller, Vehicle Control,...	The specified control algorithm is flawed	Commercial VCU controller provides brake motor control commands due to a flawed path calcuation while driving normally on a planned self-driving path	홍길동	2022-09-28 21:41	James	2022-12-21 09:37
LS-23-1		cVCU Controller, Vehicle Control,...	The specified control algorithm is flawed	Brake application due to path calculation information value output delay error	홍길동	2022-09-28 21:41	James	2022-12-21 09:37
LS-23-2		cVCU Controller, Vehicle Control,...	The specified control algorithm is flawed	Excessive operation error of brake control	홍길동	2022-09-28 21:53	James	2022-12-21 09:37
LS-24		cVCU Controller, Driver, Process M...	Controller receives incorrect feedback/inform...	When the actual location is consistent with the planned self-driving path, the driver mistakenly changes the self-driving mode. The commercial VCU controller then determines that the vehicle is controlled by the driver, and the brake...	홍길동	2022-09-28 21:41	James	2022-12-21 09:38
LS-24-1		cVCU Controller, Driver, Process M...	Controller receives incorrect feedback/inform...	Temporary autonomous-driving-off is mistaken to be the permanent one	홍길동	2022-09-28 21:41	James	2022-12-21 09:37
LS-25		cVCU Controller, Process Model	Necessary controller feedback/information d...	When driving normally on a planned autonomous path, the commercial VCU controller does not have an algorithm to handle and inform the error, providing a brake motor control command	홍길동	2022-09-28 21:41	James	2022-12-21 09:39
LS-25-1		cVCU Controller, Process Model	Necessary controller feedback/information d...	Debouncing algorithm does not exist to collect possible errors and determine their authenticity	홍길동	2022-09-28 22:20	James	2022-12-21 09:39
LS-26		cVCU Controller, CAN	Feedback/info is not received or applied to se...	When driving normally on the planned self-driving route, the vehicle information has not been updated, but cVCU controller has provided a brake motor control command	홍길동	2022-09-28 21:41	James	2022-12-21 09:39
LS-26-1		cVCU Controller, CAN	Feedback/info is not received or applied to se...	Physical failure of other controllers	홍길동	2022-09-28 21:41	James	2022-12-21 09:39
LS-26-2		cVCU Controller, CAN	Feedback/info is not received or applied to se...	Algorithm error on other controllers	홍길동	2022-09-28 22:25	James	2022-12-21 09:39
LS-27		cVCU Controller, CAN	Sensor(s) respond adequately but controller r...	When driving normally on the planned self-driving path, other controllers have updated the vehicle information appropriately and communicated via CAN	홍길동	2022-09-28 21:41	James	2022-12-21 14:47
LS-27-1		cVCU Controller, CAN	Sensor(s) respond adequately but controller r...	Corruption of CAN messages from other controllers	홍길동	2022-09-28 21:41	James	2022-12-21 14:47
LS-27-2		cVCU Controller, CAN	Sensor(s) respond adequately but controller r...	Unintended change of CAN packet order	홍길동	2022-09-28 22:27	James	2022-12-21 14:47
LS-28		cVCU Controller, CAN	Sensor(s) are not capable or not designed to...	When driving normally on the planned self-driving route, the vehicle information has been updated appropriately, but has failed to provide information to the commercial VCU controller, providing a brake motor control command	홍길동	2022-09-28 21:41	James	2022-12-21 14:48
LS-28-1		cVCU Controller, CAN	Sensor(s) are not capable or not designed to...	CAN interface open circuit/short circuit issues	홍길동	2022-09-28 21:41	James	2022-12-21 14:48
LS-229		Driver		Lack of proper understanding or education by the passenger regarding the limitations and capabilities of the autonomous driving system	Dave1	2023-03-27 17:16	Dave1	2023-03-27 17:16
LS-230		Driver		Intentional or unintentional interference with the VCU's commands, such as attempting to override the system or making sudden movements that are not aligned with the system's inputs and outputs.	Dave1	2023-03-27 17:18	Dave1	2023-03-27 17:18

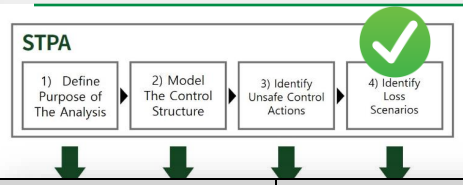
STPA on VCU System



UCA-5 cVCU Controller provides brake motor control commands when driving normally on a planned autonomous path

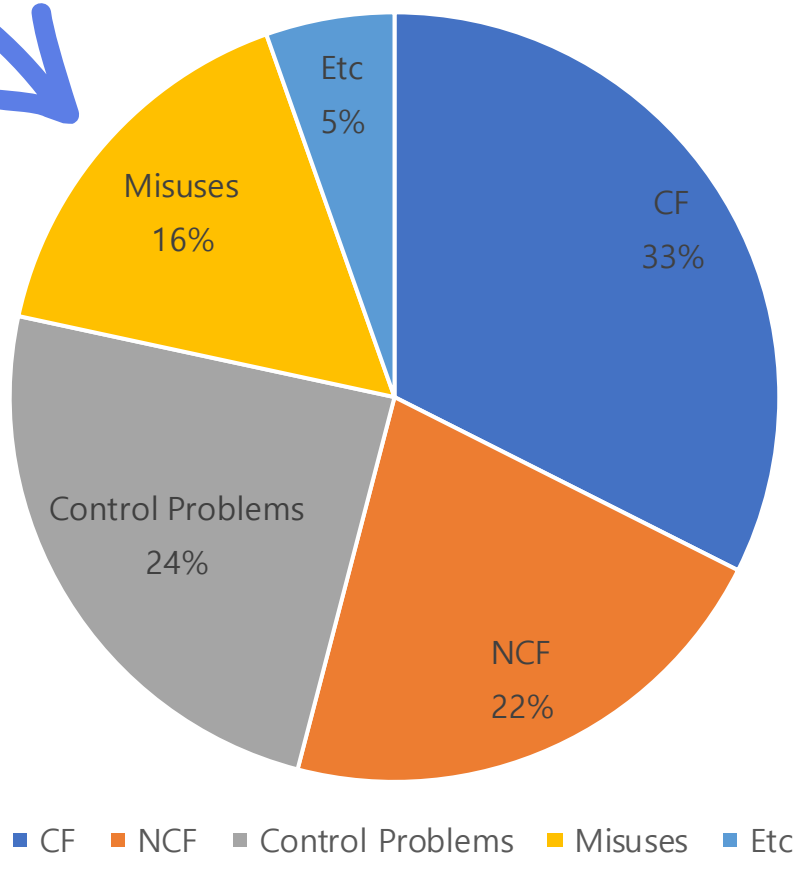


STPA on VCU System

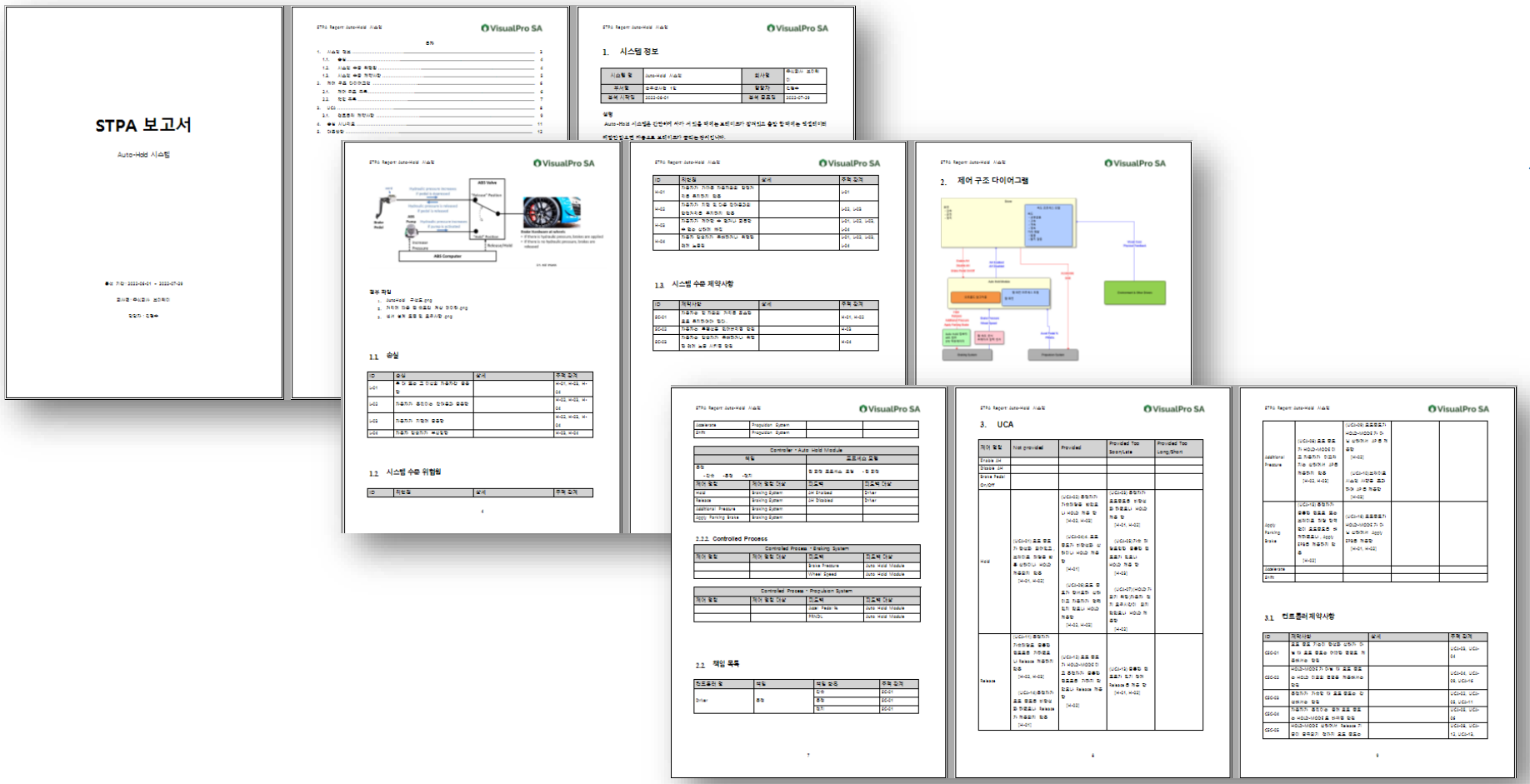


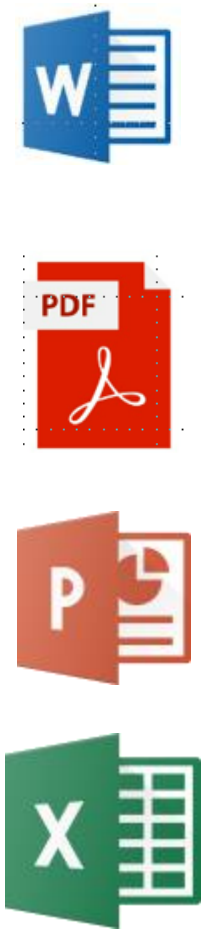
Control Action	Brake Motor Control	
UCA-5	cVCU Controller provides brake motor control commands when driving normally on a planned autonomous path	
ID	Entity	Loss Scenario
LS-21	cVCU Controller	cVCU Controller provides a brake motor control command due to a physical failure during planned autonomous driving
LS-21-1	cVCU Controller	Microprocessor (μC) with low-reliability was used
LS-22	cVCU Controller	cVCU controller provides a brake motor control command due to a power failure while driving normally on the planned self-driving path
LS-22-1	cVCU Controller	Unstable power supply (high voltage, low voltage, etc.)
LS-22-2	cVCU Controller	Power regulator with low reliability was used
LS-23	Route Calculation	Commercial VCU controller provides brake motor control commands due to a flawed path calcuation while driving normally on a planned self-driving path
LS-23-1	Route Calculation	Brake application due to path calculation information value output delay error
LS-23-2	Route Calculation	Excessive operation error of brake control
LS-24	Driver, Process Model	When the actual location is consistent with the planned self-driving path, the driver mistakenly changes the self-driving mode. The commercial VCU controller then determines that the vehicle is controlled by the driver, and the brake motor control command is provided
LS-24-1	Driver, Process Model	Temporary autonomous-driving-off is mistaken to be the permanent one
LS-25	Process Model	When driving normally on a planned autonomous path, the commercial VCU controller does not have an algorithm to handle and inform the error, providing a brake motor control command
LS-25-1	Process Model	Debouncing algorithm does not exist to collect possible errors and determine their authenticity
LS-26	cVCU Controller, CAN	When driving normally on the planned self-driving route, the vehicle information has not been updated, but cVCU controller has provided a brake motor control command
LS-26-1	cVCU Controller, CAN	Physical failure of other controllers
LS-26-2	cVCU Controller, CAN	Algorithm error on other controllers
LS-27	cVCU Controller, CAN	When driving normally on the planned self-driving path, other controllers have updated the vehicle information appropriately and communicated via CAN
LS-27-1	cVCU Controller, CAN	Corruption of CAN messages from other controllers
LS-27-2	cVCU Controller, CAN	Unintended change of CAN packet order
LS-28	cVCU Controller, CAN	When driving normally on the planned self-driving route, the vehicle information has been updated appropriately, but has failed to provide information to the commercial VCU controller, providing a brake motor control command
LS-28-1	cVCU Controller, CAN	CAN interface open circuit/short circuit issues
LS-229	Driver	Lack of proper understanding or education by the passenger regarding the limitations and capabilities of the autonomous driving system
LS-230	Driver	Intentional or unintentional interference with the VCU's commands, such as attempting to override the system or making sudden movements that are not aligned with the system's inputs and outputs.
LS-231	Driver	A passenger intentionally interferes with the VCU system by covering up sensors, disconnecting wires, or otherwise tampering with the system in order to test its safety features or cause mischief.
LS-232	Driver	A driver ignores or overrides safety alerts or warnings issued by the VCU system, either due to distraction, fatigue, or a deliberate decision to prioritize other factors, such as time or convenience.
LS-233	Process Model	VCU controller sends a command to the brake motor to stop the vehicle due to a malfunctioning battery management system.
LS-233-1	Process Model	Battery malfunction or damage
LS-233-2	Process Model	Faulty wiring or connection between the battery and the VCU
LS-233-3	Process Model	Inaccurate or misaligned battery sensor data
LS-233-4	Process Model	Insufficient error handling or contingency planning within the battery management system

Categorized

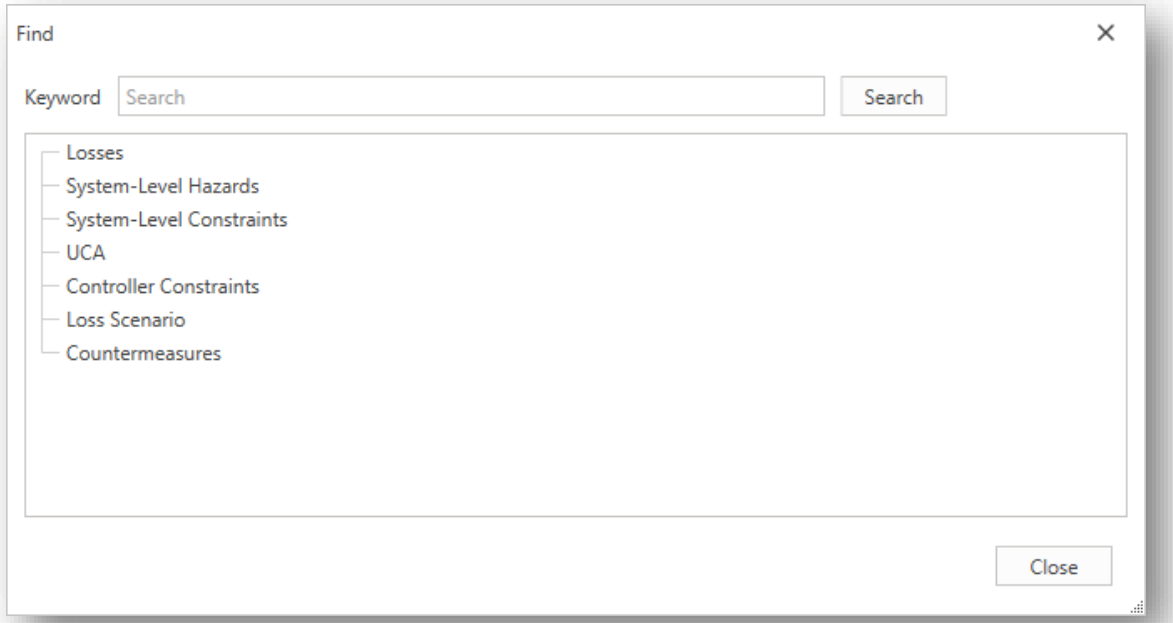


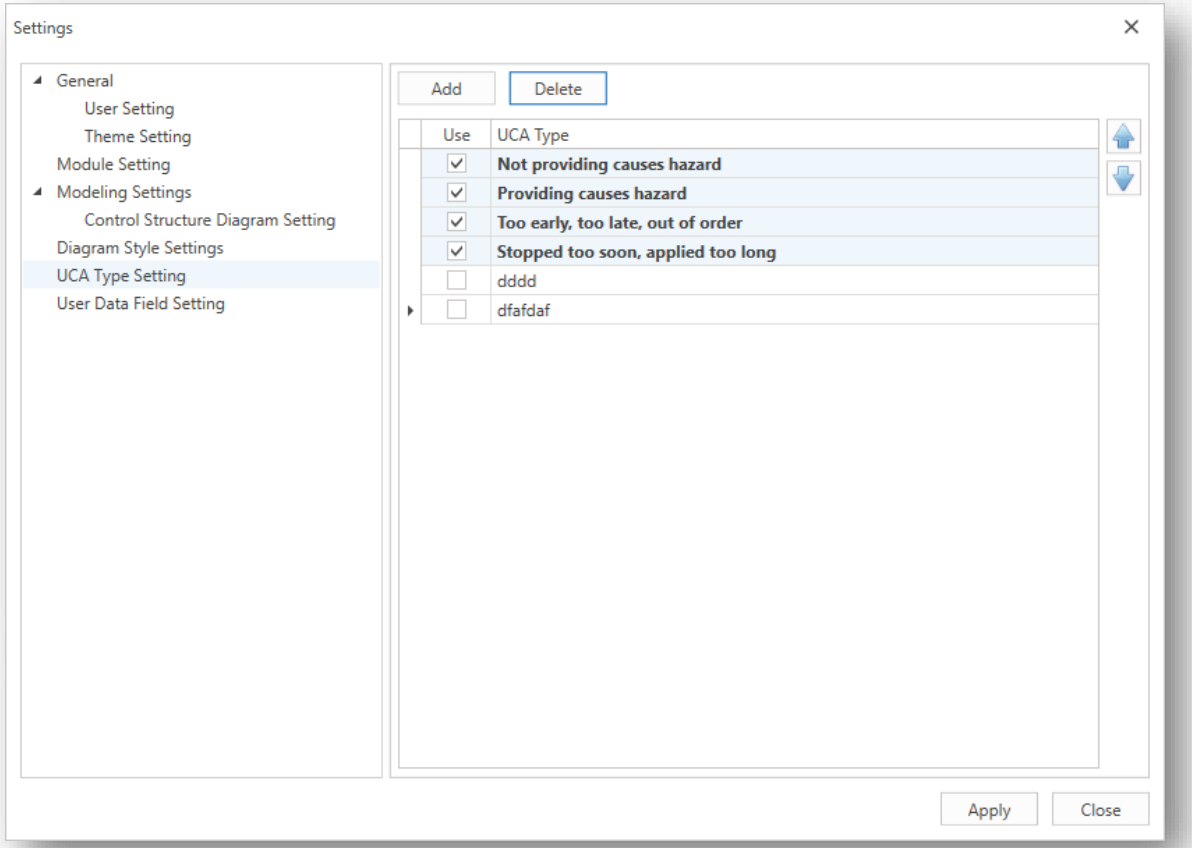
Total 37 loss scenarios was identify based on UCA-5

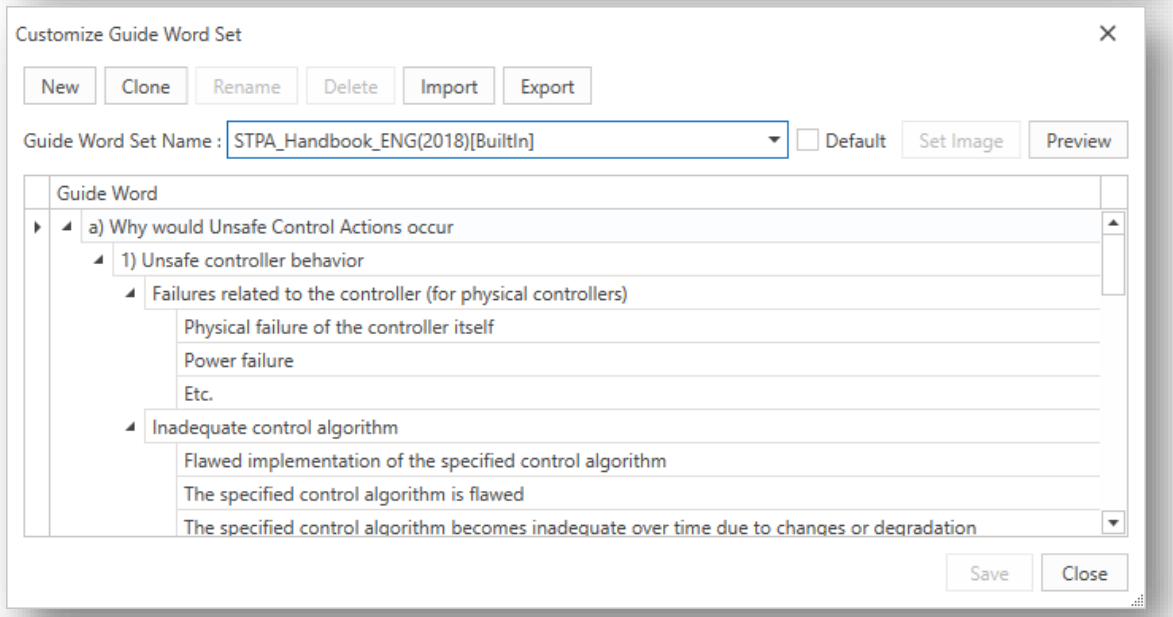




Make STPA report automatically and export to word, pdf, powerpoint and excel







We are continuously improving our tool based on customer feedbacks.

「 Contents 」

SW Safety Technologies
Global Leader

Vision

Safety

Security

VisualPro SA

Conclusion

STPA

Thank you for your attention

VWAY